Grandstream Networks, Inc.

UCM6510 IP PBX

User Manual

UCM6510 IP PBX User Manual

Index

CHANGE LOG 16

FIRMWARE VERSION 1.0.2.7 16
FIRMWARE VERSION 1.0.2.5 16
FIRMWARE VERSION 1.0.1.12 17
FIRMWARE VERSION 1.0.0.25 18

WELCOME 19

PRODUCT OVERVIEW 21

FEATURE HIGHTLIGHTS 21
TECHNICAL SPECIFICATIONS 21

INSTALLATION 25

EQUIPMENT PACKAGING 25
CONNECT YOUR UCM6510 25
CONNECT THE UCM6510 25
SAFETY COMPLIANCES 27
WARRANTY 27

GETTING STARTED 29

USE THE LCD MENU 29
USE THE LED INDICATORS 31
USE THE WEB GUI 32
ACCESS WEB GUI 32
WEB GUI CONFIGURATIONS 33
WEB GUI LANGUAGES 33
SAVE AND APPLY CHANGES 34
MAKE YOUR FIRST CALL 35

SYSTEM SETTINGS 37

USER MANAGEMENT 37
USER PRIVILEGES 37
CREATE NEW WEB UI USER 38
USER PORTAL 40
CONCURRENT MULTI-USER LOGIN 41
OPERATION LOG 41

CHANGE BINDING EMAIL *43*
NETWORK SETTINGS 44
BASIC SETTINGS *44*
802.1X *49*
STATIC ROUTES *50*
PORT FORWORDING *53*
DDNS SETTINGS *55*
FIREWALL 56
STATIC DEFENSE *56*
DYNAMIC DEFENSE *58*
FAIL2BAN *60*
CHANGE PASSWORD 61
LDAP SERVER 61
LDAP SERVER CONFIGURATIONS *62*
LDAP PHONEBOOK *63*
LDAP CLIENT CONFIGURATIONS *66*
HTTP SERVER 68
EMAIL SETTINGS 69
TIME SETTINGS 71
AUTO TIME UPDATING *71*
SET TIME MANUALLY *72*
OFFICE TIME *73*
HOLIDAY *74*
NTP SERVER 76
RECORDINGS STORAGE 77
LOGIN TIMEOUT SETTINGS 79

PROVISIONING 81

OVERVIEW 81
CONFIGURATION ARCHITECTURE FOR END POINT DEVICE 81
AUTO PROVISIONING SETTINGS 82
DISCOVERY 85
GLOBAL CONFIGURATION 86
GLOBAL POLICY *86*
GLOBAL TEMPLATES *93*
MODEL CONFIGURATION 95
MODEL TEMPLATES *95*
MODEL UPDATE *98*
DEVICE CONFIGURATION 98
CREATE NEW DEVICE *98*
MANAGE DEVICES *99*

SAMPLE APPLICATION 106

EXTENSIONS 111

CREATE NEW USER 111
CREATE NEW SIP EXTENSION 111
CREATE NEW IAX EXTENSION 117
CREATE NEW FXS EXTENSION 121
BATCH ADD EXTENSIONS 126
BATCH ADD SIP EXTENSIONS 126
BATCH ADD IAX EXTENSIONS 129
SEARCH AND EDIT EXTENSION 131
EXPORT EXTENSIONS 133
IMPORT EXTENSIONS 133
EMAIL TO USER 134

ANALOG TRUNKS 137

ANALOG TRUNKS CONFIGURATION 137
PSTN DETECTION 140
ANALOG HARDWARE CONFIGURATION 143

DIGITAL TRUNKS 147

DIGITAL HARDWARE CONFIGURATION 147
DIGITAL TRUNK CONFIGURATION 157
DIRECT OUTWARD DIALING (DOD) VIA DIGITAL TRUNKS 158
DIGITAL TRUNK TROUBLESHOOTING 158

DATA TRUNK 161

VOIP TRUNKS 163

VOIP TRUNK CONFIGURATION 163
DIRECT OUTWARD DIALING (DOD) VIA VOIP TRUNKS 173

SLA STATION 175

CREATE/EDIT SLA STATION 175
SAMPLE CONFIGURATION 176

CALL ROUTES 179

OUTBOUND ROUTES 179
INBOUND ROUTES 181
INBOUND RULE CONFIGURATIONS 182
INBOUND ROUTE: PREPEND EXAMPLE 184

BLACKLIST CONFIGURATIONS *185*

CONFERENCE BRIDGE **187**

CONFERENCE BRIDGE CONFIGURATIONS *187*
JOIN A CONFERENCE CALL *188*
INVITE OTHER PARTIES TO JOIN CONFERENCE *189*
DURING THE CONFERENCE *190*
RECORD CONFERENCE *191*

IVR **193**

CONFIGURE IVR 193
CREATE IVR PROMPT 195
RECORD NEW IVR PROMPT *195*
UPLOAD IVR PROMPT *196*

LANGUAGE SETTINGS FOR VOICE PROMPT **197**

DOWNLOAD AND INSTALL VOICE PROMPT PACKAGE 197

VOICEMAIL **201**

CONFIGURE VOICEMAIL 201
ACCESS VOICEMAIL 202
VOICEMAIL EMAIL SETTINGS 203
CONFIGURE VOICEMAIL GROUP 205

RING GROUP **207**

CONFIGURE RING GROUP 207
REMOTE EXTENSION IN RING GROUP 209

PAGING AND INTERCOM GROUP **213**

CONFIGURE PAGING/INTERCOM GROUP 213

CALL QUEUE **215**

CONFIGURE CALL QUEUE 215

EXTENSION GROUPS **219**

CONFIGURE EXTENSION GROUPS 219
USE EXTENSION GROUPS 219

PICKUP GROUPS **221**

CONFIGURE PICKUP GROUPS 221
CONFIGURE PICKUP FEATURE CODE 221

MUSIC ON HOLD 223

FAX/T.38 225

CONFIGURE FAX/T.38 225
SAMPLE CONFIGURATION TO RECEIVE FAX FROM PSTN LINE 226
SAMPLE CONFIGURATION FOR FAX-TO-EMAIL 228

ASTERISK MANAGER INTERFACE (RESTRICTED ACCESS) 229

FOLLOW ME 231

ONE-KEY DIAL 233

DISA 235

CALLBACK FEATURE 237

BLF AND EVENT LIST 239

BLF 239
EVENT LIST 239

DIAL BY NAME 243

DIAL BY NAME CONFIGURATION 243

ACTIVE CALLS AND MONITOR 247

ACTIVE CALLS STATUS 247
HANG UP ACTIVE CALLS 248
CALL MONITOR 248

CALL FEATURES 251

FEATURE CODES 251
CALL RECORDING 254
CALL PARK 255
PARK A CALL 255
RETRIEVE THE PARKED CALL 255
ENABLE SPY 256

INTERNAL OPTIONS 257

INTERNAL OPTIONS/GENERAL 257
INTERNAL OPTIONS/JITTER BUFFER 259

INTERNAL OPTIONS/RTP SETTINGS 259
INTERNAL OPTIONS/STUN MONITOR 260
IAX SETTINGS 261
IAX SETTINGS/GENERAL 261
IAX SETTINGS/REGISTRATION 261
IAX SETTINGS/STATIC DEFENSE 262
SIP SETTINGS 263
SIP SETTINGS/GENERAL 263
SIP SETTINGS/MISC 264
SIP SETTINGS/SESSION TIMER 264
SIP SETTINGS/TCP and TLS 265
SIP SETTINGS/NAT 266
SIP SETTINGS/TOS 267
VALUE-ADDED FEATURES 269
FAX SENDING 269
ANNOUNCEMENTS CENTER 269
ANNOUNCEMENTS CENTER SETTINGS 270
GROUP SETTINGS 270
STATUS AND REPORTING 273
PBX STATUS 273
TRUNKS 273
EXTENSIONS 274
QUEUES 276
CONFERENCE ROOMS 276
INTERFACES STATUS 277
DIGITAL CHANNELS STATUS 279
PARKING LOT 280
SYSTEM STATUS 281
GENERAL 282
NETWORK 282
STORAGE USAGE 283
RESOURCE USAGE 283
SYSTEM EVENTS 284
ALERT EVENTS LIST 284
ALERT LOG 286
ALERT CONTACT 288
CDR 288

DOWNLOADED CDR FILE *291*
STATISTICS *293*
RECORDING FILES *293*
CDR API CONFIGURATION FILES *294*

UPGRADING AND MAINTENANCE 301

UPGRADING 301
UPGRADING VIA NETWORK *301*
UPGRADING VIA LOCAL UPLOAD *302*
NO LOCAL FIRMWARE SERVERS *304*
BACKUP 304
BACKUP/RESTORE *305*
DATA SYNC *306*
RESTORE CONFIGURATION FROM BACKUP FILE *307*
CLEANER 308
RESET AND REBOOT 309
SYSLOG 310
TROUBLESHOOTING 311
ETHERNET CAPTURE *311*
IP PING *311*
TRACEROUTE *312*
PRI/SS7/MFC/R2 SIGNALING TRACE *313*
ANALOG RECORD TRACE *313*
E&M IMMEDIATE RECORD TRACE *314*
SERVICE CHECK *314*
REMOTE ACCESS 315
SSH ACCESS *315*

EXPERIENCING THE UCM6510 SERIES IP PBX 317

Table of Tables
UCM6510 IP PBX User Manual

Table 1: Technical Specifications 21
Table 2: UCM6510 Equipment Packaging 25
Table 3: LCD Menu Options 30
Table 4: UCM6510 LED INDICATORS 31
Table 5: User Management – Create New User 39
Table 6: Operation Log Column Header 42
Table 7: Change Binding Email option 44
Table 8: UCM6510 Network Settings->Basic Settings 44
Table 9: UCM6510 Network Settings->802.1X 50
Table 10: UCM6510 Network Settings->Static Routes 51
Table 11: UCM6510 Network Settings->Port Forwarding 53
Table 12: UCM6510 Firewall->Static Defense->Current Service 56
Table 13: Typical Firewall Settings 57
Table 14: Firewall Rule Settings 58
Table 15: UCM6510 Firewall Dynamic Defense 59
Table 16: Fail2Ban Settings 60
Table 17: HTTP Server Settings 69
Table 18: Email Settings 69
Table 19: Auto Time Updating 71
Table 20: Create New Office Time 74
Table 21: Create New Holiday 75
Table 22: Auto Provision Settings 84
Table 23: Global Policy Parameters – Localization 87
Table 24: Global Policy Parameters – Phone Settings 88
Table 25: Global Policy Parameters – Contact List 88
Table 26: Global Policy Parameters – Maintenance 90
Table 27: Global Policy Parameters – Network Settings 92
Table 28: Global Policy Parameters – Customization 92
Table 29: Create New Template 94
Table 30: Create New Model Template 96
Table 31: SIP Extension Configuration Parameters – Basic Settings 112
Table 32: SIP Extension Configuration Parameters – Media 113
Table 33: SIP Extension Configuration Parameters – Features 114
Table 34: SIP Extension Configuration Parameters – Specific Time 117
Table 35: IAX Extension Configuration Parameters – Basic Settings 117
Table 36: IAX Extension Configuration Parameters – Media 119
Table 37: IAX Extension Configuration Parameters – Features 119
Table 38: IAX Extension Configuration Parameters – Specific Time 121

Table 39: FXS Extension Configuration Parameters – Basic Settings 122
Table 40: FXS Extension Configuration Parameters – Media 123
Table 41: FXS Extension Configuration Parameters – Features 124
Table 42: FXS Extension Configuration Parameters – Specific Time 126
Table 43: Batch Add SIP Extension Parameters 126
Table 44: Batch Add IAX Extension Parameters 129
Table 45: Analog Trunk Configuration Parameters 137
Table 46: PSTN Detection for Analog Trunk 142
Table 47: Analog Hardware Configuration Parameters 144
Table 48: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE 148
Table 49: Digital Hardware Configuration Parameters: E1 - SS7 150
Table 50: Digital Hardware Configuration Parameters: E1 - MFC/R2 151
Table 51: Digital Hardware Configuration Parameters: T1/J1 - PRI_NET/PRI_CPE 153
Table 52: Digital Hardware Configuration Parameters: T1/J1 - SS7 155
Table 53: Digital Hardware Configuration Parameters: T1-E&M Immediate/E&M Wink 156
Table 54: Digital Trunk Configuration Parameters 157
Table 55: Data Trunk Configuration Parameters 162
Table 56: Create New SIP Trunk 163
Table 57: SIP Register Trunk Configuration Parameters 164
Table 58: SIP Peer Trunk Configuration Parameters 167
Table 59: Create New IAX Trunk 170
Table 60: IAX Register Trunk Configuration Parameters 171
Table 61: IAX Peer Trunk Configuration Parameters 172
Table 62: SLA Station Configuration Parameters 175
Table 63: Outbound Route Configuration Parameters 179
Table 64: Inbound Rule Configuration Parameters 182
Table 65: Conference Bridge Configuration Parameters 187
Table 66: Conference Caller IVR Menu 190
Table 67: IVR Configuration Parameters 193
Table 68: Voicemail Settings 201
Table 69: Voicemail IVR Menu 202
Table 70: Voicemail Email Settings 204
Table 71: Voicemail Group Settings 205
Table 72: Ring Group Parameters 207
Table 73: Paging/Intercom Group Configuration Parameters 213
Table 74: Call Queue Configuration Parameters 215
Table 75: FAX/T.38 Settings 225
Table 76: Follow Me Settings 232
Table 77: Follow Me Options 232
Table 78: DISA Settings 235
Table 79: Callback Configuration Parameters 237

Table 80: Event List Settings 240
Table 81: UCM6510 Feature Codes 251
Table 82: Internal Options/General 257
Table 83: Internal Options/Jitter Buffer 259
Table 84: Internal Options/RTP Settings 259
Table 85: Internal Options/STUN Monitor 260
Table 86: IAX Settings/General 261
Table 87: IAX Settings/Registration 261
Table 88: IAX Settings/Static Defense 262
Table 89: SIP Settings/General 263
Table 90: SIP Settings/Misc 264
Table 91: SIP Settings/Session Timer 264
Table 92: SIP Settings/TCP and TLS 265
Table 93: SIP Settings/NAT 266
Table 94: SIP Settings/ToS 267
Table 95: Announcements Center Settings 270
Table 96: Group Settings 270
Table 97: Trunk Status 273
Table 98: Extension Status 275
Table 99: Agent Status 276
Table 100: Interface Status Indicators 277
Table 101: Digital Channel Status Indicators 280
Table 102: Parking Lot Status 281
Table 103: System Status->General 282
Table 104: System Status->Network 282
Table 105: CDR Filter Criteria 288
Table 106: CDR Statistics Filter Criteria 293
Table 107: CDR API Configuration Files 294
Table 108: CDR API URI Parameters 295
Table 109: Network Upgrade Configuration 301
Table 110: Data Sync Configuration 307
Table 111: Cleaner Configuration 309

Table of Figures
UCM6510 IP PBX User Manual

Figure 1: UCM6510 Front View 25
Figure 2: UCM6510 Back View 25
Figure 3: UCM6510 T1/E1/J1 Crossover Cable Pin-out 26
Figure 4: UCM6510 web GUI Login Page 32
Figure 5: UCM6510 web GUI Language 34
Figure 6: UCM6510 web GUI: Apply Changes 34
Figure 7: User Management Page Display 37
Figure 8: Create New User 39
Figure 9: User Management – New Users 39
Figure 10: Edit User Information by Super Admin 40
Figure 11: User Portal Login 40
Figure 12: User Portal Layout 41
Figure 13: Multiple User Operation Error Prompt 41
Figure 14: Operation Logs 42
Figure 15: Operation Logs Filter 43
Figure 16: Change Binding Email 43
Figure 17: UCM6510 Network Interface Method: Route 47
Figure 18: UCM6510 Network Interface Method: Switch 48
Figure 19: UCM6510 Network Interface Method: Dual 49
Figure 20: UCM6510 Using 802.1X as Client 49
Figure 21: UCM6510 Using 802.1X EAP-MD5 50
Figure 22: UCM6510 Static Route Sample 52
Figure 23: UCM6510 Static Route Configuration 52
Figure 24: UCM6510 Port Forwarding Configuration 54
Figure 25: GXP2160 Web Access Using UCM6510 Port Forwarding 54
Figure 26: Register Domain Name on noip.com 55
Figure 27: UCM6510 DDNS Setting 55
Figure 28: Using Domain Name to Connect to UCM6510 56
Figure 29: Create New Firewall Rule 57
Figure 30: Configure Dynamic Defense 60
Figure 31: LDAP Server Configurations 62
Figure 32: Default LDAP Phonebook DN 63
Figure 33: Default LDAP Phonebook Attributes 63
Figure 34: Add LDAP Phonebook 64
Figure 35: Edit LDAP Phonebook 64
Figure 36: Import Phonebook 65
Figure 37: Phonebook CSV File Format 65
Figure 38: LDAP Phonebook After Import 66

Figure 39: Export Selected LDAP Phonebook 66
Figure 40: LDAP Client Configurations 67
Figure 41: GXP2200 LDAP Phonebook Configuration 68
Figure 42: UCM6510 Email Settings 70
Figure 43: UCM6510 Email Settings: Send Test Email 70
Figure 44: Set Time Manually 72
Figure 45: Create New Office Time 73
Figure 46: Settings->Time Settings->Office Time 74
Figure 47: Create New Holiday 75
Figure 48: Settings->Time Settings->Holiday 76
Figure 49: Settings->Recordings Storage 77
Figure 50: Recordings Storage Prompt Information 78
Figure 51: Recording Storage Category 78
Figure 52: Login Timeout Settings 79
Figure 53: Zero Config Configuration Architecture for End Point Device 82
Figure 54: UCM6510 Zero Config 83
Figure 55: Auto Provision Settings 84
Figure 56: Auto Discover 86
Figure 57: Discovered Devices 86
Figure 58: Global Policy Categories 87
Figure 59: Edit Global Template 94
Figure 60: Edit Model Template 97
Figure 61: Template Management 98
Figure 62: Create New Device 99
Figure 63: Manage Devices 99
Figure 64: Edit Device 100
Figure 65: Edit Customize Device Settings 102
Figure 66: Add P Value in Customize Device Settings 103
Figure 67: Modify Selected Devices–Same Model 104
Figure 68: Modify Selected Devices—Different Models 105
Figure 69: Device List in Zero Config 106
Figure 70: Zero Config Sample – Global Policy 107
Figure 71: Zero Config Sample – Device Preview 1 108
Figure 72: Zero Config Sample – Device Preview 2 109
Figure 73: Zero Config Sample – Device Preview 3 110
Figure 74: Create New Device 111
Figure 75: Manage Extensions 132
Figure 76: Export Extensions 133
Figure 77: Export Extensions 133
Figure 78: Email To User: Prompt Information 134
Figure 79: Email To User: Account Registration Information and QR Code 135

Figure 80: Email To User: LDAP Client Information and QR Code 135
Figure 81: UCM6510 FXO Tone Settings 140
Figure 82: UCM6510 PSTN Detection 141
Figure 83: UCM6510 PSTN Detection: Auto Detect 141
Figure 84: UCM6510 PSTN Detection: Semi-Auto Detect 142
Figure 85: FXS Ports Signaling Preference 143
Figure 86: FXO Ports ACIM Settings 144
Figure 87: Digital Hardware Configuration 147
Figure 88: Troubleshooting Digital Trunks 159
Figure 89: Data Trunk Web Page 161
Figure 90: Data Trunk Configuration 161
Figure 91: DOD extension selection 174
Figure 92: Edit DOD 174
Figure 93: SLA Station 175
Figure 94: Enable SLA Mode for Analog Trunk 176
Figure 95: Analog Trunk with SLA Mode Enabled 176
Figure 96: SLA Example - SLA Station 177
Figure 97: SLA Example - MPK Configuration 177
Figure 98: Inbound Route feature: Prepend 185
Figure 99: Blacklist Configuration Parameters 185
Figure 100: Conference Invitation From web GUI 189
Figure 101: Conference Recording 191
Figure 102: Click On Prompt To Create IVR Prompt 195
Figure 103: Record New IVR Prompt 195
Figure 104: Upload IVR Prompt 196
Figure 105: Language Settings for Voice Prompt 198
Figure 106: Voice Prompt Package List 198
Figure 107: New Voice Prompt Language Added 199
Figure 108: Voicemail Email Settings 204
Figure 109: Voicemail Group 205
Figure 110: Ring Group 207
Figure 111: Ring Group Configuration 209
Figure 112: Sync LDAP Server option 210
Figure 113: Manually Sync LDAP Server 210
Figure 114: Ring Group Remote Extension 211
Figure 115: Paging/Intercom Group 213
Figure 116: Page/Intercom Group Settings 214
Figure 117: Call Queue 215
Figure 118: Agent Login Settings 218
Figure 119: Edit Extension Group 219
Figure 120: Select Extension Group in Outbound Route 220

Figure 121: Edit Pickup Group 221
Figure 122: Edit Pickup Feature Code 222
Figure 123: Music On Hold Default Class 223
Figure 124: Configure Analog Trunk without Fax Detection 226
Figure 125: Configure Extension For Fax Machine 227
Figure 126: Configure Inbound Rule for Fax 227
Figure 127: Create Fax Extension 228
Figure 128: Inbound Route to Fax Extension 228
Figure 129: Create Follow Me 231
Figure 130: Edit Follow Me 231
Figure 131: Configure One-Key Dial 233
Figure 132: One-Key Dial Destinations 234
Figure 133: Create New DISA 235
Figure 134: Create New Event List 240
Figure 135: Create Dial By Name Group 243
Figure 136: Dial By Name Group In IVR Key Pressing Events 244
Figure 137: Dial By Name Group In Inbound Route 244
Figure 138: Configure Extension First Name and Last Name 245
Figure 139: Status->PBX Status->Active Calls - Ringing 247
Figure 140: Status->PBX Status->Active Calls – Call Established 247
Figure 141: Configure to Monitor an Active Call 248
Figure 142: Download Recording File from CDR Page 255
Figure 143: Fax Sending in Web UI 269
Figure 144: Announcements Center 270
Figure 145: Announcements Center Group Configuration 271
Figure 146: Announcements Center Code Configuration 272
Figure 147: Announcements Center example 272
Figure 148: Status->PBX Status 273
Figure 149: Trunk Status 273
Figure 150: Extension Status 275
Figure 151: Queue Status 276
Figure 152: Conference Room Status 277
Figure 153: Digital Channels Status 280
Figure 154: Parking Lot Status 281
Figure 155: System Status->Storage Usage 283
Figure 156: System Status->Resource Usage 284
Figure 157: System Events->Alert Events Lists: Disk Usage 284
Figure 158: System Events->Alert Events Lists: Modify Admin Password 285
Figure 159: System Events->Alert Events Lists: Memory Usage 285
Figure 160: System Events->Alert Events Lists: System Reboot 285
Figure 161: System Events->Alert Events Lists: System Update 286

Figure 162: System Events->Alert Events Lists: System Crash 286
Figure 163: System Events->Alert Log 286
Figure 164: System Events->Alert Log 287
Figure 165: Filter for Alert Log 287
Figure 166: CDR Filter 288
Figure 167: Call Report 289
Figure 168: Call Report Entry with Audio Recording File 290
Figure 169: Automatic Download Settings 290
Figure 170: Downloaded CDR File Sample - Call To Shows "s" 291
Figure 171: Downloaded CDR File Sample - Source Channel and Dest Channel 1 291
Figure 172: Downloaded CDR File Sample - Source Channel and Dest Channel 2 292
Figure 173: Downloaded CDR File Sample - Source Channel and Dest Channel 3 292
Figure 174: CDR Statistics 293
Figure 175: Network Upgrade 301
Figure 176: Local Upgrade 302
Figure 177: Upgrading Firmware Files 303
Figure 178: Reboot UCM6510 303
Figure 179: Create New Backup 305
Figure 180: Backup / Restore 306
Figure 181: Local Backup 306
Figure 182: Data Sync 307
Figure 183: Restore UCM6510 from Backup File 308
Figure 184: Cleaner 309
Figure 185: Reset and Reboot 310
Figure 186: Ethernet Capture 311
Figure 187: PING 312
Figure 188: Traceroute 312
Figure 189: Troubleshooting Analog Trunks 313
Figure 190: E&M Immediate Record Trace 314
Figure 191: Service Check 314
Figure 192: SSH Access 315

CHANGE LOG

This section documents significant changes from previous versions of the UCM6510 user manual. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

FIRMWARE VERSION 1.0.2.7

- Added PRI T310 configuration [Table 48: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE]
- Added Announcements Center [ANNOUNCEMENTS CENTER]

FIRMWARE VERSION 1.0.2.5

- Added option to enable/disable SSH access via LCD or web UI [SSH ACCESS]
- Added ability to select voicemail storage (Email + WAV is supported) [Table 70: Voicemail Email Settings]
- Added support to allow remote peer extensions in ring group [REMOTE EXTENSION IN RING GROUP]
- Added ability to strip and prepend digits in inbound routes [Table 64: Inbound Rule Configuration Parameters]
- Added ability to search extensions on Extension page [
- SEARCH AND EDIT EXTENSION]
- Added user portal for users to log in with extension number, access user information, extension configuration and CDR [USER PORTAL]
- Added support to send Fax via web UI [FAX SENDING]
- Added “Enable LDAP” option to skip the extension from UCM default LDAP phonebook [Table 31: SIP Extension Configuration Parameters]
- Added video RE-INVITE support
- Added DDNS Support [DDNS SETTINGS]
- Added support for Call Barging using feature codes [ENABLE SPY]
- Added ability to search the CDR by called number [Table 105: CDR Filter Criteria]
- Added ability to select the file types for automatic backup [BACKUP/RESTORE]
- Added automatic backup support on SD Card or USB storage [BACKUP/RESTORE]
- Added support to skip trunk authentication by time condition [Table 33: SIP Extension Configuration Parameters – Features]
- Added option to send P-Asserted-Identity header in SIP Register Trunk [Table 57: SIP Register Trunk Configuration Parameters]

- Added ability to specify trunks in CDR filters [CDR]
- Added ability to use Pattern in Caller Number to filter CDR [CDR]
- Added support to send UNREGISTER when VoIP trunk is disabled [Table 57: SIP Register Trunk Configuration Parameters]
- Added LDAP client support [LDAP CLIENT CONFIGURATIONS]
- Added option to specify the chronological order to voice mails [Table 68: Voicemail Settings]
- Added option to configure whether to skip pressing ½ to accept or reject calls from Follow Me [Table 76: Follow Me Settings]
- Added option to specify port range in Port Forwarding configuration [Table 11: UCM6510 Network Settings->Port Forwarding]
- Added ability to go back to IVR menu from Dial By Name by pressing the star key [DIAL BY NAME CONFIGURATION]
- Added support to upgrade SIP end device via SD card in Zero Config [Table 26: Global Policy Parameters – Maintenance]
- Added ability to filter alert logs [ALERT LOG]
- Added ability to delete alert logs [ALERT LOG]
- Added NAT option for peer trunk [Table 63: Outbound Route Configuration Parameters]
- Improved Automatic Download CDR result format [CDR]
- Fixed Digital Trunk SS7 signaling mode inbound / outbound call problem
- Fixed Asterisk is crashed while using external MCB and CEI

FIRMWARE VERSION 1.0.1.12

- Added Active Calls feature to monitor call status and barge in active calls [ACTIVE CALLS AND MONITOR]
- Added support to disable the trunk for VoIP trunk and analog trunk [Table 56: Create New SIP Trunk] [Table 45: Analog Trunk Configuration Parameters]
- Added RBS support on T1
- Added Frame Relay support on Data Trunk [DATA TRUNK]
- Added 'Assign CIC to D-channel' option on SS7 settings page [Table 49: Digital Hardware Configuration Parameters: E1 - SS7]
- Added 'First CIC' option in SS7 configuration [Table 49: Digital Hardware Configuration Parameters: E1 - SS7]
- Added 'D-Chan' selection for PRI and SS7 in editing digital ports [Table 48: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE] [Table 49: Digital Hardware Configuration Parameters: E1 - SS7]
- Added support for Ring simultaneously feature for extensions [Table 31: SIP Extension Configuration Parameters]
- Added support for Music On Hold selection per extension [Table 31: SIP Extension Configuration Parameters]

- Added support to disable this extension per extension [Table 31: SIP Extension Configuration Parameters]
- Added ability to set personal password for making outbound calls per extension [Table 31: SIP Extension Configuration Parameters]
- Added 'TEL URI' configuration for SIP extension/VoIP trunk [Table 31: SIP Extension Configuration Parameters] [Table 56: Create New SIP Trunk]
- Added E&M Immediate and E&M Wink signaling for T1
- Renamed the 'network backup' settings items to 'data sync' [DATA SYNC]
- Added "Download Search Result" in CDR [CDR]
- Added office time and holiday setting support [OFFICE TIME] [HOLIDAY]
- Added time condition for call forward [EXTENSIONS]
- Added support to monitor FXO trunk using SLA [SLA STATION]
- Added One-Key Dial function [ONE-KEY DIAL]
- Added Follow Me support [FOLLOW ME]
- Supported external number as the key pressing event of an IVR
- Improved APIs for Zero Config templates and settings [PROVISIONING]
- Supported GXP16XX, Surveillance and GS_wave models in Zero Config [PROVISIONING]
- Added advanced settings for devices discovered in Zero Config [DEVICE CONFIGURATION]
- Added ability to delete multiple recording files at one time [RECORDING FILES]
- Added call queue destination if no answer/timeout [Table 74: Call Queue Configuration Parameters]
- Added call queue Music on Hold customization [Table 74: Call Queue Configuration Parameters]
- Added restricted AMI access [ASTERISK MANAGER INTERFACE (RESTRICTED ACCESS)]
  Warning: Please do not enable AMI on the UCM6510 if it is placed on a public or untrusted network unless you have taken steps to protect the device from unauthorized access. It is crucial to understand that AMI access can allow AMI user to originate calls and the data exchanged via AMI is often very sensitive and private for your UCM6510 system. Please be cautious when enabling AMI access on the UCM6510 and restrict the permission granted to the AMI user. By using AMI on UCM6510 you agree you understand and acknowledge the risks associated with this.
- Added ability to choose the type(s) of files to be cleaned in cleaner [CLEANER]
- Added DTMF configuration per SIP trunk [Table 56: Create New SIP Trunk]
- Added ability to upload and play ring group announcement [Table 72: Ring Group Parameters]
- Added ability to upload and play paging call announcement [PAGING AND INTERCOM GROUP]
- Added Alert-info configuration for distinctive ringing on inbound route [Table 64: Inbound Rule Configuration Parameters]
- Added ability to prepend digits/trunk name to inbound calls' caller ID [Table 64: Inbound Rule Configuration Parameters]
- Modified Static Routes Interface display when network method is changed [STATIC ROUTES]

FIRMWARE VERSION 1.0.0.25

- This is the initial version.

WELCOME

Thank you for purchasing Grandstream UCM6510 IP PBX appliance. The UCM6510 is an innovative IP PBX appliance for E1/T1/J1 networks that brings enterprise-grade unified communications and security protection to enterprises, small-to-medium businesses (SMBs), retail environments and residential settings in an easy-to-manage fashion. Powered by an advanced hardware platform and revolutionary software functionalities, the UCM6510 offers a breakthrough turnkey solution for converged voice, video, data, fax, security surveillance, and mobility applications out of the box without any extra license fees or recurring costs.

Caution:

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

Warning:

Please do not use a different power adapter with the UCM6510 as it may cause damage to the products and void the manufacturer warranty.

This document is subject to change without notice. The latest electronic version of this user manual is available for download here:
http://www.grandstream.com/support

Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

This page intentionally left blank

PRODUCT OVERVIEW

FEATURE HIGHTLIGHTS

- 1 GHz quad-core Cortex A9 application processor, large memory (1GB DDR3 RAM, 32GB Flash), and dedicated high performance multi-core DSP array for advanced voice processing
- 1 Integrated 1 T1/E1/J1 interface, 2 PSTN trunk FXO ports, 2 analog telephone/Fax FXS ports with lifeline capability in case of power outage, and up to 50 SIP trunk accounts
- Hardware DSP based 128ms-tail-length carrier-grade line echo cancellation (LEC), hardware based caller ID/call progress tone and smart automated impedance matching for various countries
- Gigabit network port(s) with integrated PoE, USB, SD card; integrated NAT router with advanced QoS support
- Strong defense against malicious attacks (Fail2ban, Whitelist, Blacklist, alerts, etc.)
- Data communication via T1/E1/J1 and data-voice combined communication via T1/E1/J1 with SS7 or PRI
- Supports up to 2000 SIP endpoint registrations, up to 200 concurrent calls (up to 100 SRTP encrypted concurrent calls), and up to 64 conference attendees
- Flexible dial plan, call routing, site peering, call recording (manual and automatic per SIP call and SIP trunk), central control panel for endpoints, integrated NTP server, and integrated LDAP contact directory
- Automated detection and provisioning of IP phones, video phones, ATAs, gateways, SIP cameras, and other endpoints for easy deployment
- Strongest-possible security protection using SRTP, TLS, and HTTPS with hardware encryption accelerator
- Redundant power supply, advanced support for Hot Standby Clustering and High Availability to minimize system down time (pending)
- Automatic export of previous day's data; periodically cleans up user data

TECHNICAL SPECIFICATIONS

Table 1: Technical Specifications

Interfaces	
Analog Telephone FXS Ports	2 RJ11 ports (both with lifeline capability in case of power outage)
PSTN Line FXO Ports	2 RJ11 ports (both with lifeline capability in case of power outage)
T1/E1/J1 Interface	1 RJ45 port
Network Interfaces	Dual Gigabit ports (switched or routed) with PoE; A 3rd Gigabit port for Hot-Standby Clustering
NAT Router	Yes (user configurable)

Peripheral Ports	USB, SD
LED Indicators	Power ½, PoE, USB, SD, T1/E1/J1, FXS ½, FXO ½, LAN, WAN, Cluster Heartbeat
LCD Display	128x32 dot matrix graphic LCD with DOWN and OK buttons
Reset Switch	Yes, long press for factory reset and short press for reboot
Voice/Video Capabilities	
Voice-over-Packet Capabilities	LEC with NLP Packetized Voice Protocol Unit, 128ms-tail-length carrier grade Line Echo Cancellation, Dynamic Jitter Buffer, Modem detection and auto-switch to G.711
Voice and Fax Codecs	G.711 A-law/U-law, G.722, G.723.1 5.3K/6.3K, G.726, G.729A/B, Ilbc, GSM, AAL2-G.726-32, ADPCM; T.38
Video Codecs	H.264, H.263, H.263+
QoS	Layer 3 QoS, Layer 2 QoS
Signaling and Control	
DTMF Methods	In Audio, RFC2833, and SIP INFO
Digital Signaling	PRI, SS7, MFC/R2, E&M
Provisioning Protocol and Plug-and-Play	TFTP/HTTP/HTTPS, auto-discovery & auto-provisioning of Grandstream IP endpoints via ZeroConfig (DHCP Option 66/multicast SIP SUBSCRIBE/Mdns), eventlist between local and remote trunks
Network Protocols	TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, SIP (RFC3261), STUN, SRTP, TLS, LDAP, HDLC, HDLC-ETH, PPP, Frame Relay
Disconnect Methods	Call Progress Tone, Polarity Reversal, Hook Flash Timing, Loop Current Disconnect, Busy Tone
Security	
Media	SRTP, TLS, HTTPS, SSH
Advanced Defense	Fail2ban, alert events, Whitelist, Blacklist, strong password based access control
Physical	
Universal Power Supply	Input: 100-240VAC, 50-60Hz; Output: DC+12VDC, 1.5A
Physical	Unit Weight: 2.165 KG; Package weight: 3.012 KG
Dimensions	440mm (L) x 185mm (W) x 44mm (H)
Environmental	Operating: 32 – 113°F / 0 – 45°C, Humidity 10-90% (non-condensing) Storage: 14 – 140°F / -10 – 60°C, Humidity 10-90% (non-condensing)
Mounting	Rack mount and Desktop

Additional Features	
Multi-language Support	English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, German, Russian, Italian, Polish, Czech for web GUI; Customizable IVR/voice prompts for English, Chinese, British English, German, Spanish, Greek, French, Italian, Dutch, Polish, Portuguese, Russian, Swedish, Turkish, Hebrew and Arabic
Caller ID	Bellcore/Telcordia, ETSI-FSK, ETSI-DTMF, SIN 227 – BT, NTT Japan (pending)
Polarity Reversal/ Wink	Yes, with enable/disable option upon call establishment and termination
Call Center	Multiple configurable call queues, automatic call distribution (ACD) based on agent skills/availability/busy level, in-queue announcement
Customizable Auto Attendant	Up to 5 layers of IVR (Interactive Voice Response)
Maximum Call Capacity	Up to 2000 registered SIP endpoints, up to 200 concurrent calls
Conference Bridges	Up to 8 bridges, up to 64 simultaneous conference attendees
Call Features	Call park, call forward, call transfer, DND, DISA, ring group, pickup group, blacklist, paging/intercom and etc
Compliance	• FCC: Part 15 (CFR 47) Class B, Part 68 • CE: EN55022 Class B, EN55024, EN61000-3-2, EN61000-3-3, EN60950-1, TBR21, RoHS • A-TICK: AS/NZS CISPR 22 Class B, AS/NZS CISPR 24, AS/NZS 60950, AS/ACIF S002 • ITU-T K.21 (Basic Level); UL 60950 (power adapter) • T1: TIA-968-B Section 5.2.4 • E1: TBR12/TBR13, E1: AS/ACIF

INSTALLATION

Before deploying and configuring the UCM6510 series, the device needs to be properly powered up and connected to network. This section describes detailed information on installation, connection and warranty policy of the UCM6510 series.

EQUIPMENT PACKAGING

Table 2: UCM6510 Equipment Packaging

Main Case	Yes (x 1)
Power Adapter	Yes (x 2)
Ethernet Cable	Yes (x 1)
Wall Mount	Yes (x 2)
Screws	Yes (x 6)
Quick Installation Guide	Yes (x 1)

CONNECT YOUR UCM6510

CONNECT THE UCM6510

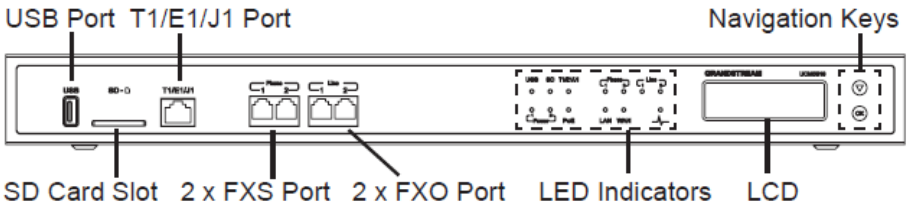


Figure 1: UCM6510 Front View

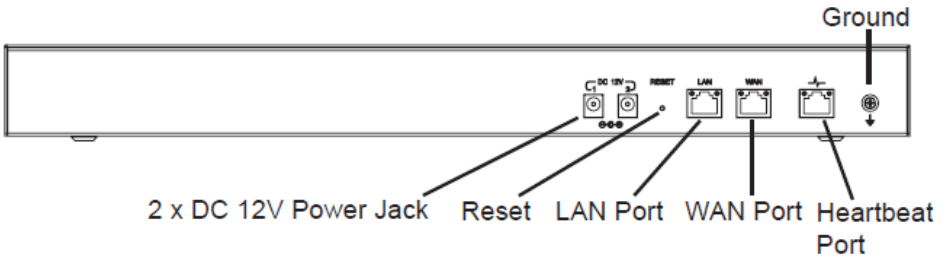


Figure 2: UCM6510 Back View

Follow the steps below to connect the UCM6510 for initial setup:

1. Connect one end of an RJ-45 Ethernet cable (cable type: straight through) into the WAN port of the UCM6510; connect the other end into the uplink port of an Ethernet switch/hub.
2. Connect the 12V DC power adapter into the DC 12V power jack 1 on the back of the UCM6510. Insert the main plug of the power adapter into a surge-protected power outlet. (Connect the second power adapter into the DC 12V power jack 2 for failover purpose in case the first one is down).
3. Wait for the UCM6510 to boot up. The LCD in the front will show its hardware information when the bootup process is done.
4. Once the UCM6510 is successfully connected to the network, the LED indicator for the WAN port in the front will be in solid green and the LCD shows up the IP address.

Depending on how the UCM6510 is used, users can follow the steps below for optional setup:

1. PSTN Line Connection: connect PSTN lines from the wall jack to the UCM6510 LINE ports (FXO ports).
2. Analog Line Connection: connect analog lines (phone and fax) to the PHONE ports (FXS ports).
3. T1/E1/J1 Line Connection: connect one end of the T1/E1/J1 cable provided from the service provider into the T1/E1/J1 port of the UCM6510; connect the other end into the T1/E1/J1 wall jack. T1/E1/J1 crossover cable should be used and it's not provided in the UCM6510 package. Please see T1/E1/J1 crossover cable pin-out in the figure below:

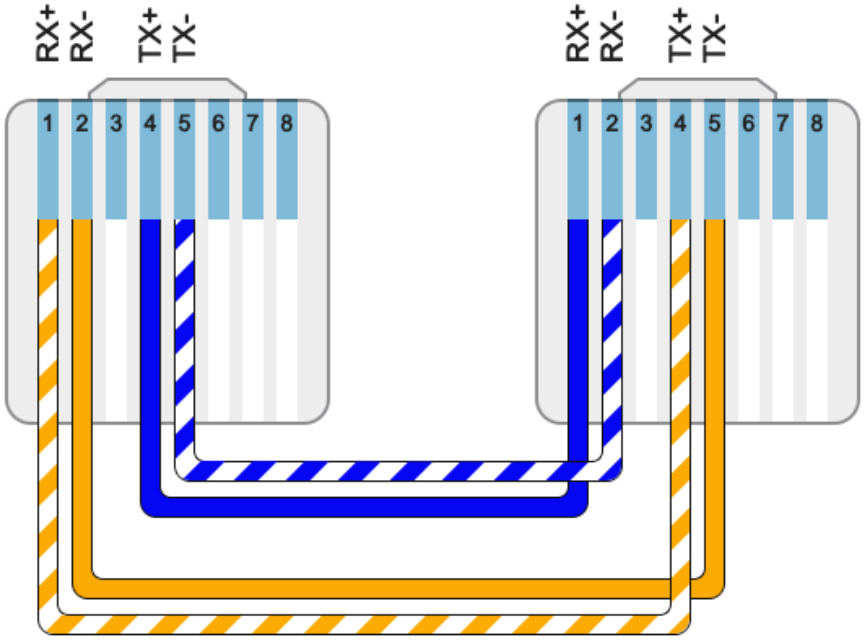


Figure 3: UCM6510 T1/E1/J1 Crossover Cable Pin-out

SAFETY COMPLIANCES

The UCM6510 series IP PBX complies with FCC/CE and various safety standards. The UCM6510 power adapter is compliant with the UL standard. Use the universal power adapter provided with the UCM6510 package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

WARRANTY

If the UCM6510 series IP PBX was purchased from a reseller, please contact the company where the device was purchased for replacement, repair or refund. If the device was purchased directly from Grandstream Networks, contact our Technical Support Team for a RMA (Return Materials Authorization) number before the product is returned. Grandstream Networks reserves the right to remedy warranty policy without prior notification.

⚠ **Warning:**

Use the power adapter provided with the UCM6510 series IP PBX. Do not use a different power adapter as this may damage the device. This type of damage is not covered under warranty.

This page intentionally left blank

GETTING STARTED

The UCM6510 provides LCD interface, LED indication and web GUI configuration interface.

- The LCD displays hardware, software and network information. Users could also navigate in the LCD menu for device information and basic network configuration.
- The LED indication at the front of the device provides interface connection and activity status.
- The web GUI gives users access to all the configurations and options for UCM6510 setup.

This section provides step-by-step instructions on how to use the LCD menu, LED indicators and web GUI of the UCM6510. Once the basic settings are done, users could start making calls from UCM6510 extension registered on a SIP phone as described at the end of this section.

USE THE LCD MENU

- **Default LCD Display**
  By default, when the device is powered up, the LCD will show device model (e.g., UCM6510), hardware version (e.g., V1.4A) and IP address. Press “Down” button and the system time will be displayed (e.g., 2014-10-21 14:20).

- **Menu Access**
  Press “OK” button to start browsing menu options. Please see menu options in [Table 3: LCD Menu Options].

- **Menu Navigation**
  Press the “Down” arrow key to browser different menu options. Press the “OK” button to select an entry.

- **Exit**
  If “Back” option is available in the menu, select it to go back to the previous menu. For “Device Info” “Network Info” and “Web Info” which do not have “Back” option, simply press the “OK” button to go back to the previous menu. Additionally, the LCD will display default idle screen after staying in menu option for 15 seconds.

- **LCD Backlight**
  The LCD backlight will be on upon key pressing. The backlight will go off after the LCD stays in idle for 30 seconds.

The following table shows the LCD menu options.

Table 3: LCD Menu Options

View Events	• **Critical Events** • **Other Events**
Device Info	• **Hardware**: Hardware version number • **Software**: Software version number • **P/N**: Part number • **WAN MAC**: WAN side MAC address • **LAN MAC**: LAN side MAC address • **Uptime**: System up time since the last reboot
Network Info	• **WAN Mode**: DHCP, Static IP, or PPPoE • **WAN IP**: IP address • **WAN Subnet Mask** • **LAN IP**: IP address • **LAN Subnet Mask**
Network Menu	• **WAN Mode**: Select WAN mode as DHCP, Static IP or PPPoE • **Static Routes Reset**: Click to reset the static route setting
Factory Menu	• **Reboot** • **Factory Reset** • **LCD Test Patterns** Press “OK” to start. Then press “Down” button to test different LCD patterns. When done, press “OK” button to exit. • **Fan Mode** Select “Auto” or “On”. • **LED Test Patterns** Select “All On” “All Off” or “Blinking” and check LED status for USB, SD, T1/E1/J1, Phone 1/Phone 2, Line 1/Line 2 ports. After the LED test, select “Back” in the menu and the device will show the LED actual status again. • **RTC Test Patterns** Select “2022-02-22 22:22” or “2011-01-11 11:11” to start the RTC (Real-Time Clock) test pattern. Check the system time from LCD idle screen by pressing “DOWN” button, or from web GUI->**System Status**->**General** page. After the test, reboot the device manually and the device will display the correct

	time. • **Hardware Testing** Select "Test SVIP" to perform SVIP test on the device. This is mainly for factory testing purpose which verifies the hardware connection inside the device. The diagnostic result displays on the LCD after the test is done.
Web Info	• **Protocol**: Web access protocol. HTTP or HTTPS. By default it's HTTPS • **Port**: Web access port number. By default it's 8089
SSH Switch	• **Enable SSH:** Enable SSH access. • **Disable SSH:** Disable SSH access. By default the SSH access is disabled.

USE THE LED INDICATORS

The UCM6510 has LED indicators in the front to display connection status. The following table shows the status definitions.

Table 4: UCM6510 LED INDICATORS

LED Indicator	LED Status
Power 1/Power 2 PoE LAN WAN USB SD Phone 1 /Phone 2 (FXS) Line 1/Line 2 FXO	**Solid**: Connected **Fast Blinking**: Data Transferring **Slow Blinking**: Trying to connect **OFF**: Not Connected
T1/E1/J1	**Solid**: Connected and working **Fast Blinking (0.5s on/0.5s off)**: No cable is connected; or connected but the link is not working at all. **Slow Blinking (1s on/1s off)**: Connected but the link is only working one-way

USE THE WEB GUI

ACCESS WEB GUI

The UCM6510 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE (version 8+), Mozilla Firefox, Google Chrome and etc.

Figure 4: UCM6510 web GUI Login Page

To access the web GUI:

1. Connect the computer to the same network as the UCM6510.
2. Ensure the device is properly powered up and shows its IP address on the LCD.
3. Open a web browser on the computer and enter the IP address in the address bar. The web login page will display as shown above.
4. Enter the administrator's login and password to access the web configuration menu. The default administrator's username and password is "admin" and "admin". It is highly recommended to change the default password after login for the first time.

⚠ **Note:**

By default, the UCM6510 has “Redirect From Port 80” enabled. Therefore, if users type in the UCM6510 IP address in the web browser, the web page will be automatically redirected to the page using HTTPS and port 8089.

For example, if the LCD shows 192.168.40.167, please enter 192.168.40.167 in your web browser and the web page will be redirected to:

https://192.168.40.167:8089

The option “Redirect From Port 80” can be configured under the UCM6510 web GUI->**Settings**->**HTTP Server**.

WEB GUI CONFIGURATIONS

There are four main sections in the web GUI for users to view the PBX status, configure and manage the PBX.

- **Status:** Displays PBX status, System Status, System Events and CDR.
- **PBX:** To configure extensions, trunks, call routes, zero config for auto provisioning, call features, internal options, IAX settings, SIP settings, as well as ports configuration for digital trunks.
- **Settings:** To configure network settings, firewall settings, change password, LDAP Server, HTTP Server, Email Settings, Time Settings and NTP server.
- **Maintenance**: To perform firmware upgrade, backup configurations, cleaner setup, reset/reboot, syslog setup and troubleshooting.

WEB GUI LANGUAGES

Currently the UCM6510 web GUI supports the following languages:

English
Simplified Chinese
Traditional Chinese
Spanish

French
Portuguese
Russian
Italian
Polish
German

Users can select the displayed language in web GUI login page, or at the upper right of the web GUI after logging in.

Figure 5: UCM6510 web GUI Language

SAVE AND APPLY CHANGES

Click on “Save” button after configuring the web GUI options in one page. After saving all the changes, make sure click on “Apply Changes” button on the upper right of the web page to submit all the changes. If the change requires reboot to take effect, a prompted message will pop up for you to reboot the device.

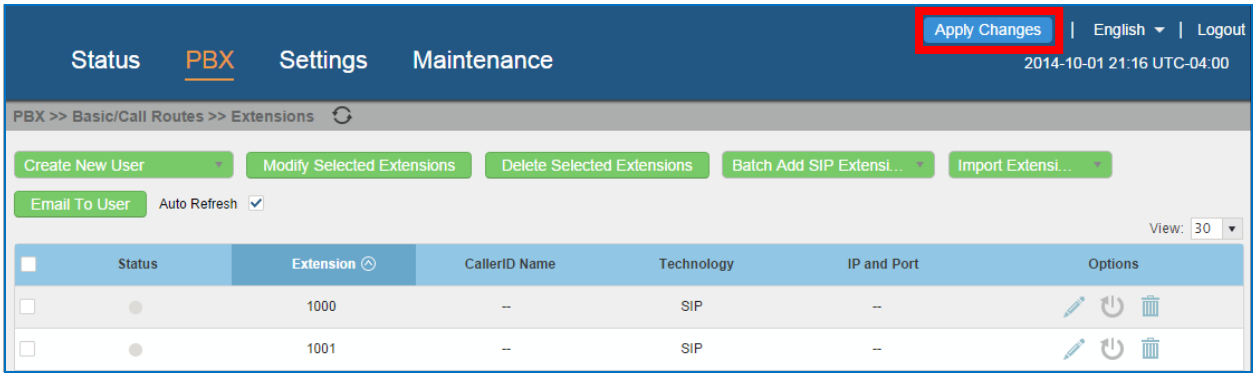


Figure 6: UCM6510 web GUI: Apply Changes

MAKE YOUR FIRST CALL

Power up the UCM6510 and your SIP end point phone. Connect both devices to the network. Then follow the steps below to make your first call.

1. Log in the UCM6510 web GUI, go to **PBX**->**Basic/Call Routes**->**Extensions**.
2. Click on “Create New SIP Extension” to create a new extension. You will need User ID, Password and Voicemail Password information to register and use the extension later.
3. Register the extension on your phone with the SIP User ID, SIP server and SIP Password information. The SIP server address is the UCM6510 IP address.
4. When your phone is registered with the extension, dial *97 to access the voicemail box. Enter the Voicemail Password once you hear “Password” voice prompt.
5. Once successfully logged in to the voicemail, you will be prompted with the Voice Mail Main menu.
6. You are successfully connected to the PBX system now.

This page intentionally left blank

SYSTEM SETTINGS

This section explains configurations for system-wide parameters on the UCM6510. Those parameters include Network Settings, Firewall, Change Password, LDAP server, HTTP server, Email settings, Time Settings and NTP Server settings.

USER MANAGEMENT

User management is on web GUI->**Settings**->**User Management** page. User could create multiple accounts for different administrators to log in the UCM6510 web GUI. Additionally the system will automatically create user accounts along with creating new extensions for extension users to login to the web UI using their extension number and password. All existing user accounts for web UI login will be displayed on User Management page as shown in the following figure.

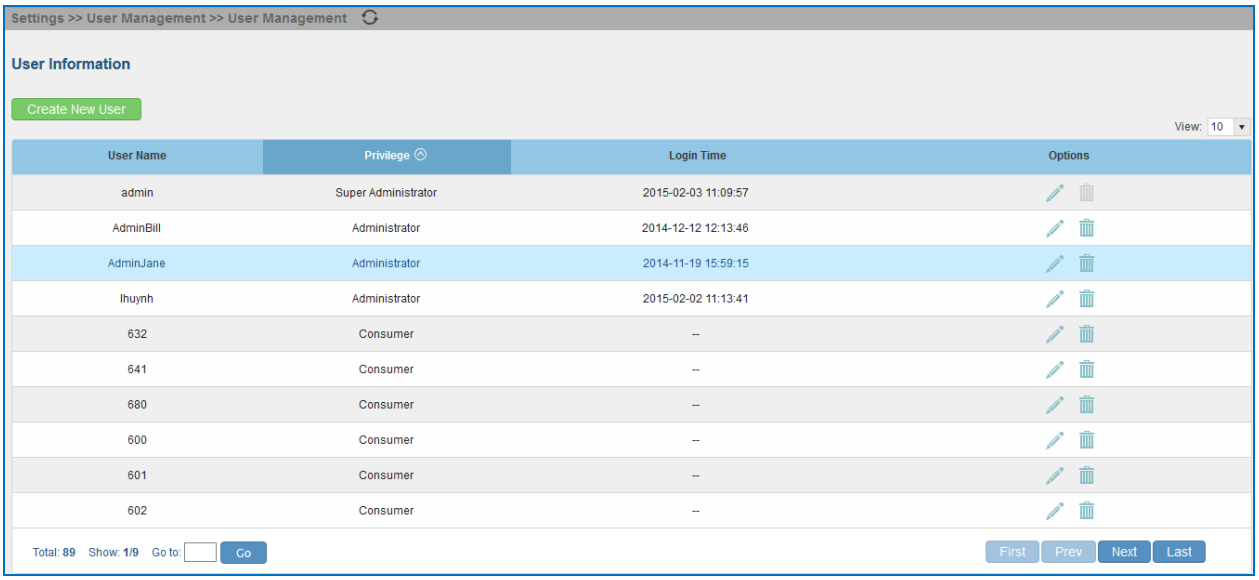


Figure 7: User Management Page Display

USER PRIVILEGES

Three privilege levels are supported:

- **Super Admin**

  - This is the highest privilege. Super Admin can access all pages on UCM6510 web GUI, change

configuration for all options and execute all the operations.
- Super Admin can create, edit and delete one or more users with “Admin” privilege
- Super Admin can edit and delete one or more users with “Consumer” privilege
- Super Admin can view operation logs generated by all users.
- By default, the user account “admin” is configured with “Super Admin” privilege and it’s the only user with “Super Admin” privilege. The User Name and Privilege level cannot be changed or deleted.
- Super Admin could change its own login password on web UI->**Settings**->**Change Password** page.
- Super Admin could view operations done by all the users in web UI->**Settings**->**User Management**->**Operation Log**.

- **Admin**

  - Users with “Admin” privilege can only be created by “Super Admin” user.
  - “Admin” privilege users are not allowed to access the following pages:
    Maintenance->**Upgrade**
    Maintenance->**Backup**
    Maintenance->**Cleaner**
    Maintenance->**Reset/Reboot**
    Settings->**User Management**->**Operation Log**
  - “Admin” privilege users cannot create new users for login.

- **Consumer**

  - A user account for web UI login is created automatically by the system when a new extension is created.
  - The user could log in the web UI with the extension number and password to access user information, extension configuration and CDR of that extension.

CREATE NEW WEB UI USER

When logged in as Super Admin, click on

to create a new account for web UI user. The following dialog will prompt. Configure the parameters as shown in below table.

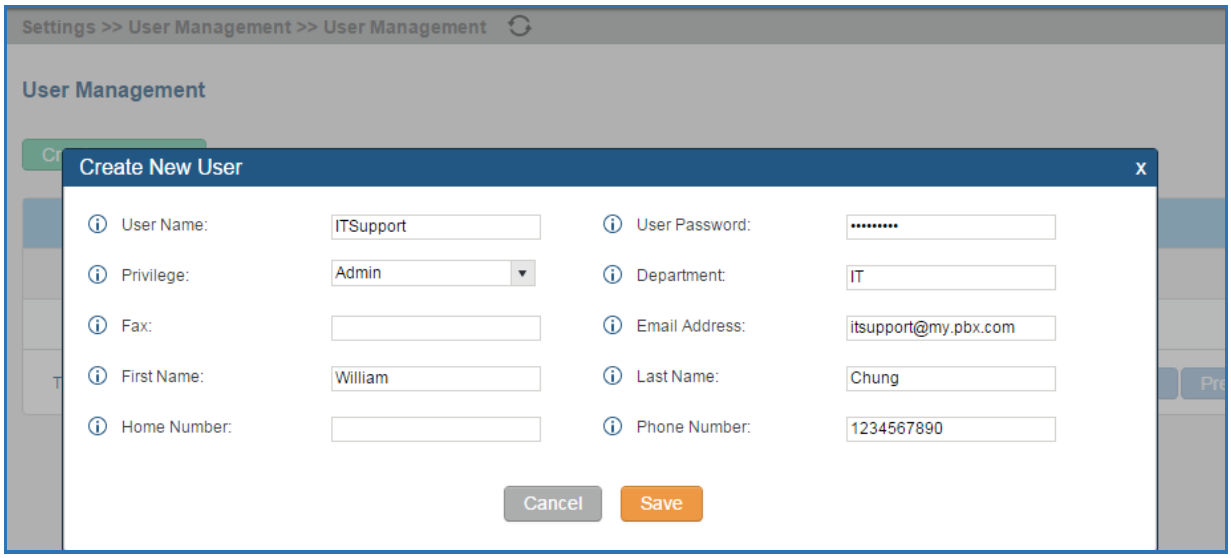


Figure 8: Create New User

Table 5: User Management – Create New User

User Name	Configure a username to identify the user which will be required in web UI login. Letters, digits and underscore are allowed in the user name.
User Password	Configure a password for this user which will be required in web UI login. Letters, digits and underscore are allowed.
Privilege	This is the role of the web UI user. Currently only “Admin” is supported when Super Admin creates a new user.
Department	Enter the necessary information to keep a record for this user.
Fax	
Email Address	
First Name	
Last Name	
Home Number	
Phone Number	

Once created, the Super Admin can edit the users by clicking on or delete the user by clicking on .

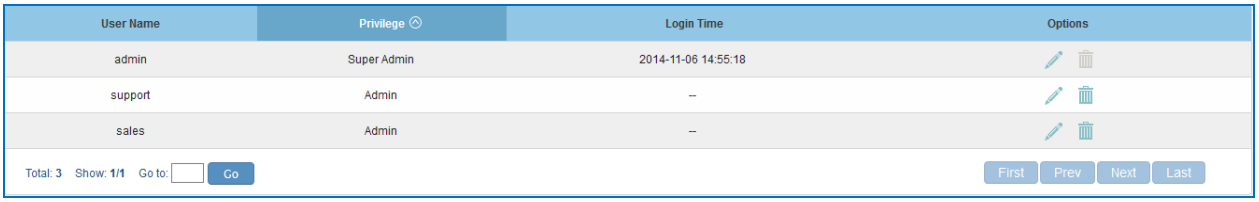


Figure 9: User Management – New Users

USER PORTAL

The user could log in web UI user portal using the extension number and password. When there is an extension created in the UCM6510, the corresponding user account for the extension is automatically created. The user portal allows limited access including user information, extension configuration and CDR information of the extension. The login username is the extension number and the password is configured by Super Admin. The following figure shows the dialog of editing the account information by Super Admin. The User Name must be the extension number and it's not configurable.

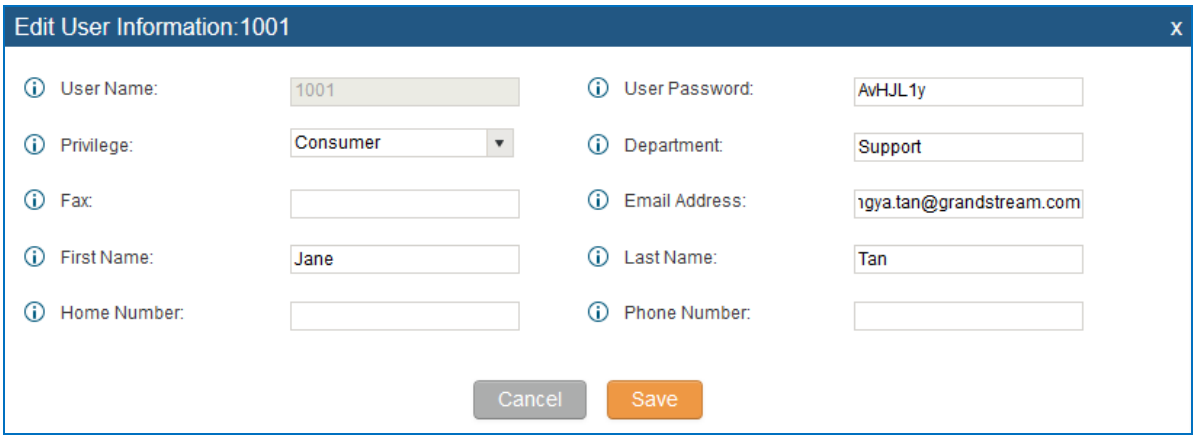


Figure 10: Edit User Information by Super Admin

The following figure shows an example of login page using extension number 1000 as the username.

Figure 11: User Portal Login

After login, the web UI displays is shown as below.

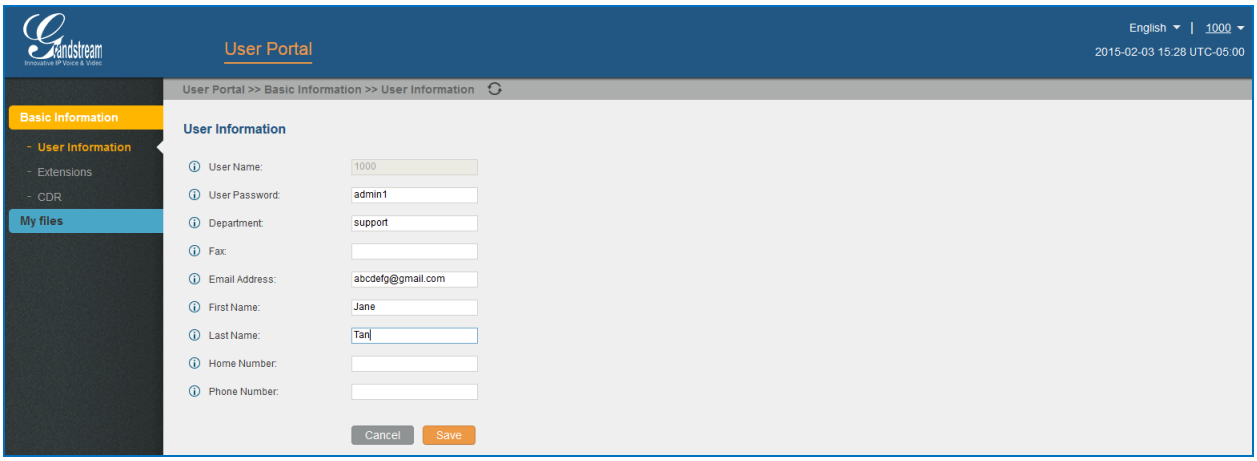


Figure 12: User Portal Layout

For the configuration parameter information in each page, please refer ***[Table 5: User Management – Create New User]*** for options in **User Portal**->**Basic Information**->**User Information** page; please refer to ***[EXTENSIONS]*** for options in **User Portal**->**Basic Information**->**Extension** page; please refer to ***[CDR]*** for **User Portal**->**Basic Information**->**CDR** page.

CONCURRENT MULTI-USER LOGIN

When there are multiple web UI users created, concurrent multi-user login is supported on the UCM6510. Multiple users could edit options and have configurations take effect simultaneously. However, if different users are editing the same option or making the same operation (by clicking on “Apply Changes”), a prompt will pop up as shown in the following figure.

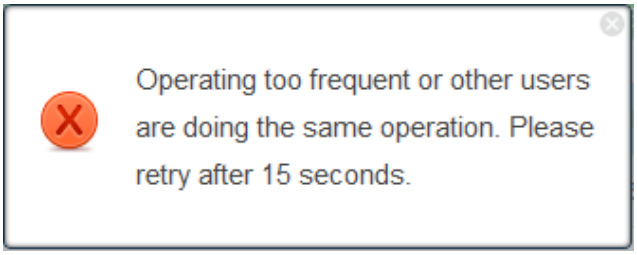
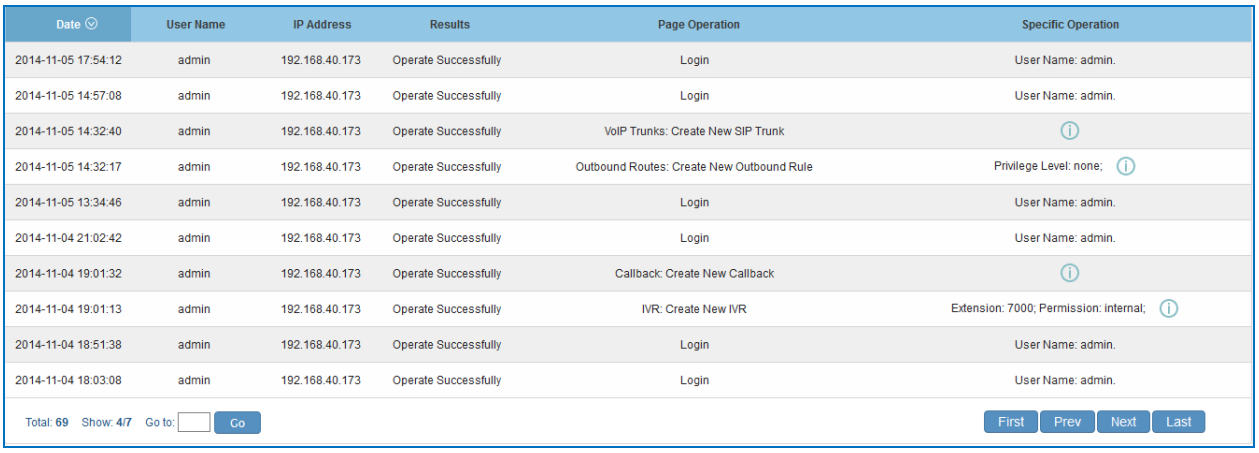


Figure 13: Multiple User Operation Error Prompt

OPERATION LOG

Super Admin has the authority to view operation logs on UCM6510 web GUI->**Settings**->**User Management**->**Operation Log** page. Operation logs list operations done by all the web UI users, for example, web UI login, creating trunk, creating outbound rule and etc. There are 6 columns to record the operation details “Date”, “User Name”, “IP Address”, “Results”, “Page Operation” and “Specific Operation”.



Date	User Name	IP Address	Results	Page Operation	Specific Operation
2014-11-05 17:54:12	admin	192.168.40.173	Operate Successfully	Login	User Name: admin.
2014-11-05 14:57:08	admin	192.168.40.173	Operate Successfully	Login	User Name: admin.
2014-11-05 14:32:40	admin	192.168.40.173	Operate Successfully	VoIP Trunks: Create New SIP Trunk	
2014-11-05 14:32:17	admin	192.168.40.173	Operate Successfully	Outbound Routes: Create New Outbound Rule	Privilege Level: none;
2014-11-05 13:34:46	admin	192.168.40.173	Operate Successfully	Login	User Name: admin.
2014-11-04 21:02:42	admin	192.168.40.173	Operate Successfully	Login	User Name: admin.
2014-11-04 19:01:32	admin	192.168.40.173	Operate Successfully	Callback: Create New Callback	
2014-11-04 19:01:13	admin	192.168.40.173	Operate Successfully	IVR: Create New IVR	Extension: 7000; Permission: internal;
2014-11-04 18:51:38	admin	192.168.40.173	Operate Successfully	Login	User Name: admin.
2014-11-04 18:03:08	admin	192.168.40.173	Operate Successfully	Login	User Name: admin.

Total: 69 Show: 4/7 Go to: Go First Prev Next Last

Figure 14: Operation Logs

The operation log can be sorted and filtered for easy access. Click on the header of each column to sort. For example, clicking on “Date” will sort the logs according to operation date and time. Clicking on “Date” again will reverse the order.

Table 6: Operation Log Column Header

Date	The date and time when the operation is executed.
User Name	The username of the user who performed the operation.
IP Address	The IP address from which the operation is made.
Results	The result of the operation.
Page Operation	The page where the operation is made. For example, login, logout, delete user, create trunk and etc.
Specific Operation	Click on ⓘ to view the options and values configured by this operation.

User could also filter the operation logs by time condition, IP address and/or username. Configure these conditions and then click on View Operation Logs.

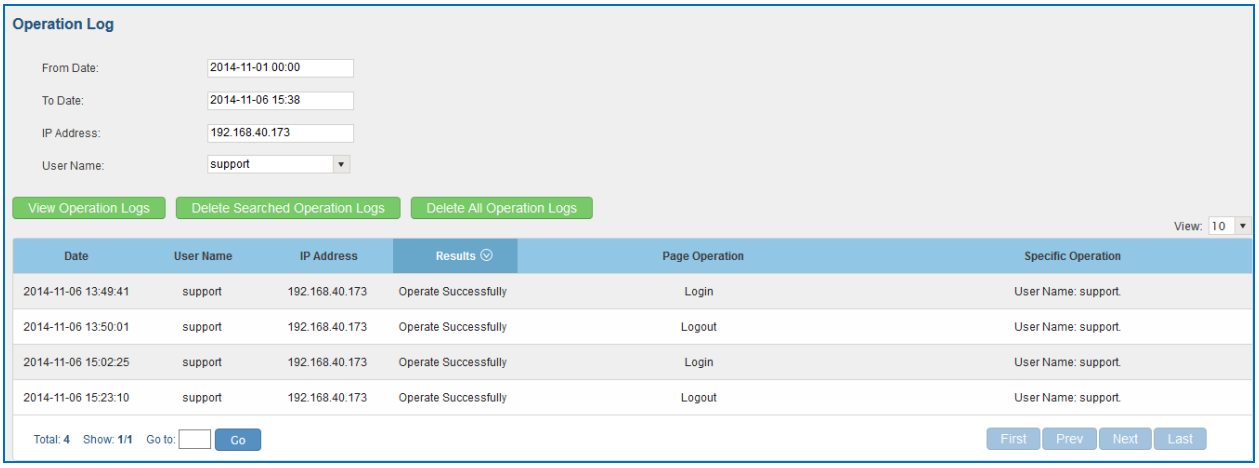


Figure 15: Operation Logs Filter

The above figure shows an example that operations made by user "support" on device with IP 192.168.40.173 from 2014-11-01 00:00 to 2014-11-06 15:38 are filtered out and displayed.

To delete operation logs, users can perform filtering first and then click on Delete Searched Operation Logs to delete the filtered result of operation logs. Or users can click on Delete All Operation Logs to delete all operation logs at once.

CHANGE BINDING EMAIL

UCM6510 allows user to configure binding email in case login password is lost. UCM6510 login credential will be sent to the designated email address. The feature can be found under web UI->**Settings**->**User Management**->**Change Binding Email**.

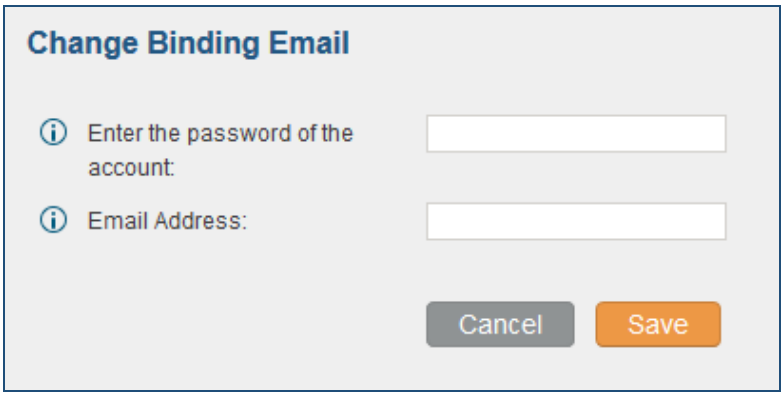


Figure 16: Change Binding Email

Table 7: Change Binding Email option

Enter the password of the account	Enter the current login user credential for UCM6510
Email Address	Email Address is used to retrieve password when password is lost

NETWORK SETTINGS

After successfully connecting the UCM6510 to the network for the first time, users could log in the web GUI and go to **Settings**->**Network Settings** to configure the network parameters for the device. Select each tab in web GUI->**Settings**->**Network Settings** page to configure LAN/WAN settings, 802.1X and Port Forwarding.

⚠ **Note:**

To connect the UCM6510 to network, T1/E1/J1 data trunk can also be used, instead of using the WAN/LAN port. Please see section ***[DATA TRUNK]*** to use UCM6510 data trunk to connect the device to Internet.

BASIC SETTINGS

Please refer to the following tables for basic network configuration parameters on the UCM6510.

Table 8: UCM6510 Network Settings->Basic Settings

Method	Select “Route”, “Switch” or “Dual” mode on the network interface of UCM6510. The default setting is “Route”. • **Route** WAN port interface will be used for uplink connection. LAN port interface will be used to serve as router. • **Switch** WAN port interface will be used for uplink connection. LAN port interface will be used as bridge for PC connection. • **Dual** Both ports can be used for uplink connection. Users will need assign LAN 1 or LAN 2 as the default interface in option “Default Interface” and configure “Gateway IP” for this interface if static IP is used for the interface.
Preferred DNS Server	Enter the preferred DNS server address. If Preferred DNS is configured, the

	UCM6510 will use it as Primary DNS server.
WAN (when "Method" is set to "Route")	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings. The default setting is 0.0.0.0.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
User Name	Enter the user name to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for WAN port. The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for WAN port. The default value is 0.
LAN (when Method is set to "Route")	
IP Address	Enter the IP address assigned to LAN port. The default setting is 192.168.2.1.
Subnet Mask	Enter the subnet mask. The default setting is 255.255.255.0.
DHCP Server Enable	Enable or disable DHCP server capability. The default setting is "Yes".
DNS Server 1	Enter DNS server address 1. The default setting is 8.8.8.8.
DNS Server 2	Enter DNS server address 2. The default setting is 208.67.222.222.
Allow IP Address From	Enter the DHCP IP Pool starting address. The default setting is 192.168.2.100.
Allow IP Address To	Enter the DHCP IP Pool ending address. The default setting is 192.168.2.254.
Default IP Lease Time	Enter the IP lease time (in seconds). The default setting is 43200.
LAN (when Method is set to "Switch")	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings. The default setting is 0.0.0.0.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
User Name	Enter the user name to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for LAN port. The default value is 0.

Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for LAN port. The default value is 0.
LAN 1 / LAN 2 (when Method is set to "Dual")	
Default Interface	If "Dual" is selected as "Method", users will need assign the default interface to be LAN 1 (mapped to UCM6510 WAN port) or LAN 2 (mapped to UCM6510 LAN port) and then configure network settings for LAN 1 and LAN 2. The default interface is LAN 2.
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160.
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings when the port is assigned as default interface. The default setting is 0.0.0.0.
DNS Server 1	Enter the DNS server 1 address for static IP settings. The default setting is 0.0.0.0.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
User Name	Enter the user name to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for LAN port. The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for LAN port. The default value is 0.

- **Method: Route**

  WAN port interface is used for uplink connection; LAN port interface is used as a router. Please see a sample diagram below.

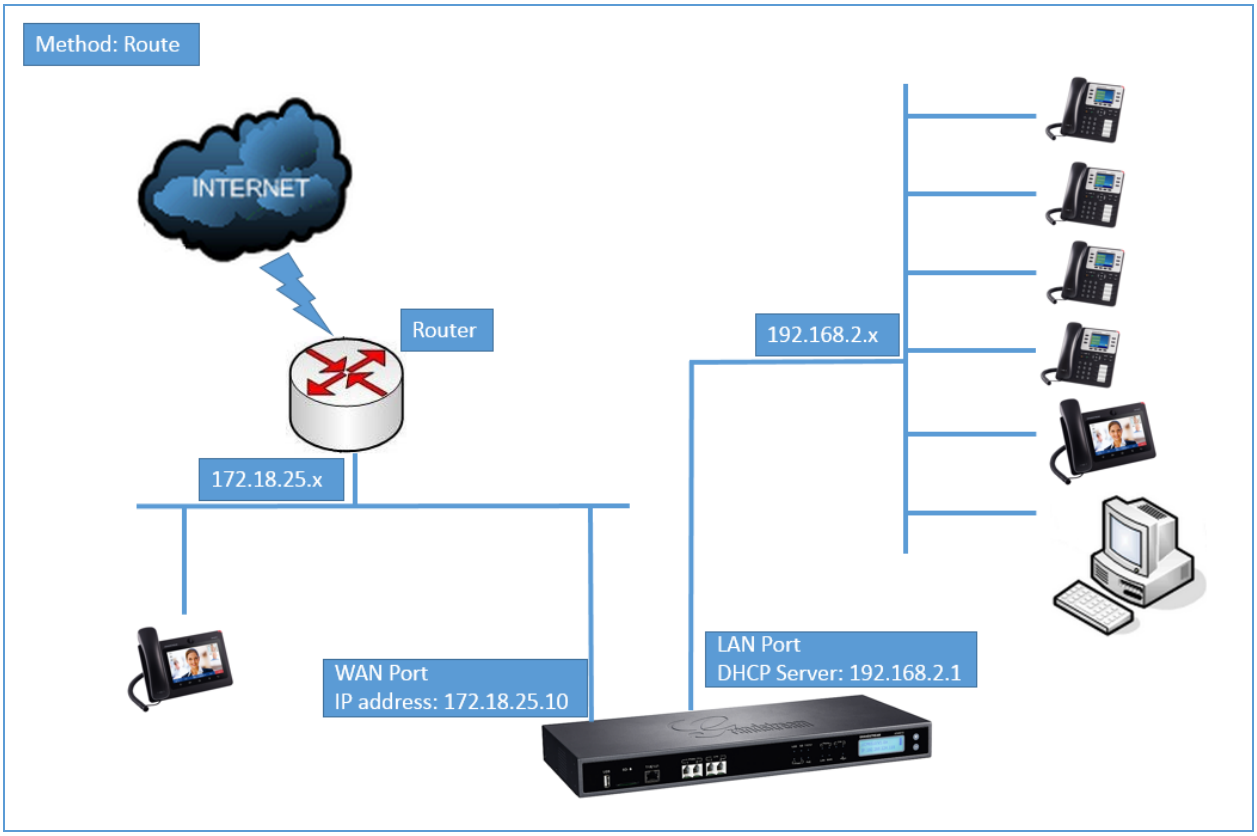


Figure 17: UCM6510 Network Interface Method: Route

- **Method: Switch**

  WAN port interface is used for uplink connection; LAN port interface is used as bridge for PC connection.

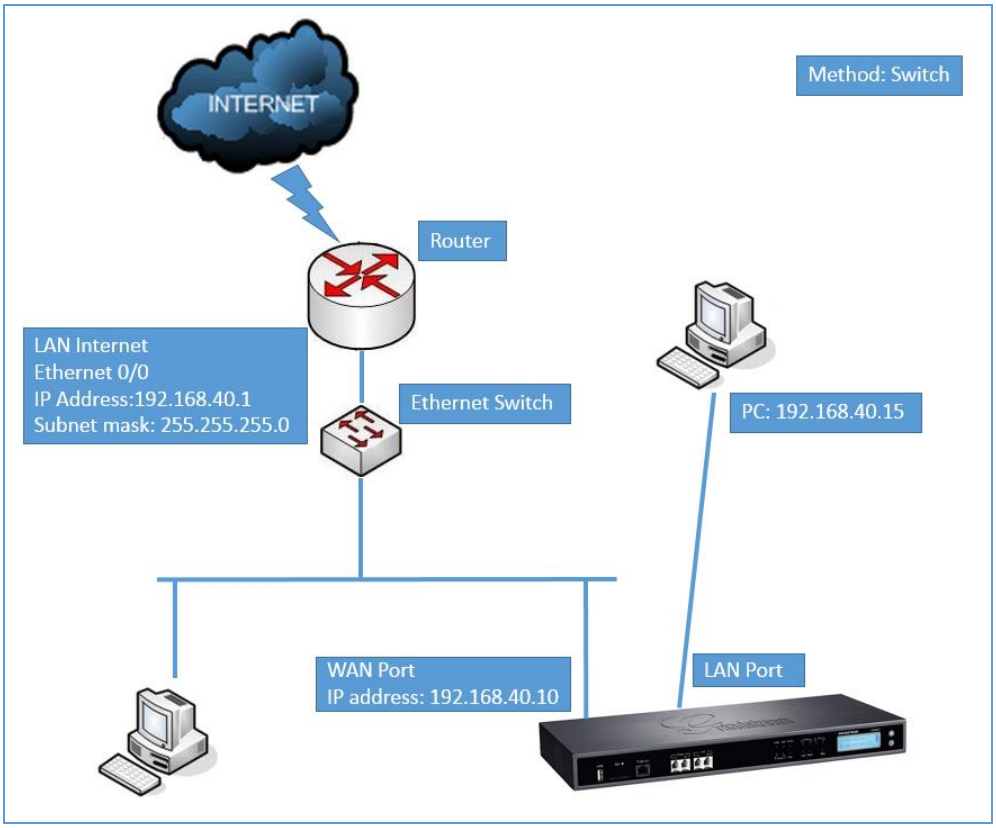


Figure 18: UCM6510 Network Interface Method: Switch

- **Method: Dual**

  Both WAN port and LAN port are used for uplink connection. WAN port will be mapped to LAN 1 interface; LAN port will be mapped to LAN 2 interface. Users will need assign LAN 1 or LAN 2 as the default interface in option “Default Interface” and configure “Gateway IP” if static IP is used for this interface.

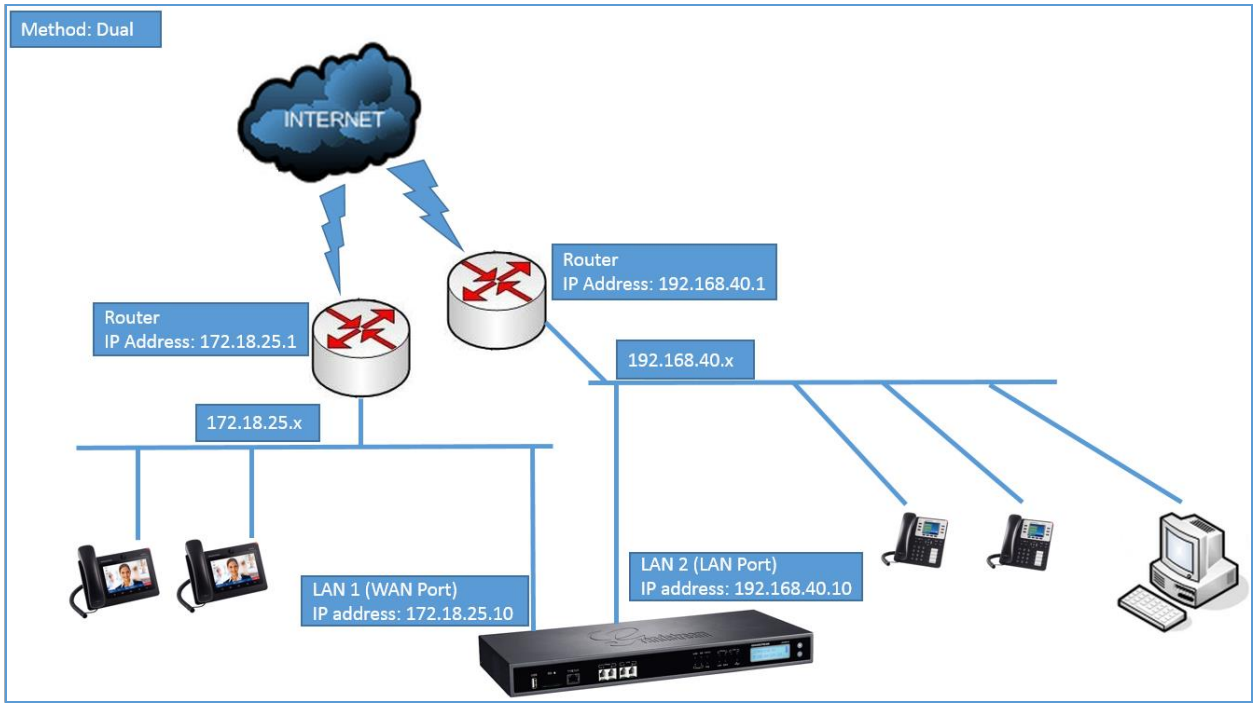


Figure 19: UCM6510 Network Interface Method: Dual

802.1X

IEEE 802.1X is an IEEE standard for port-based network access control. It provides an authentication mechanism to device before the device is allowed to access Internet or other LAN resources. The UCM6510 supports 802.1X as a supplicant/client to be authenticated. The following diagram and figure show UCM6510 uses 802.1X mode "EAP-MD5" on WAN port as client in the network to access Internet.

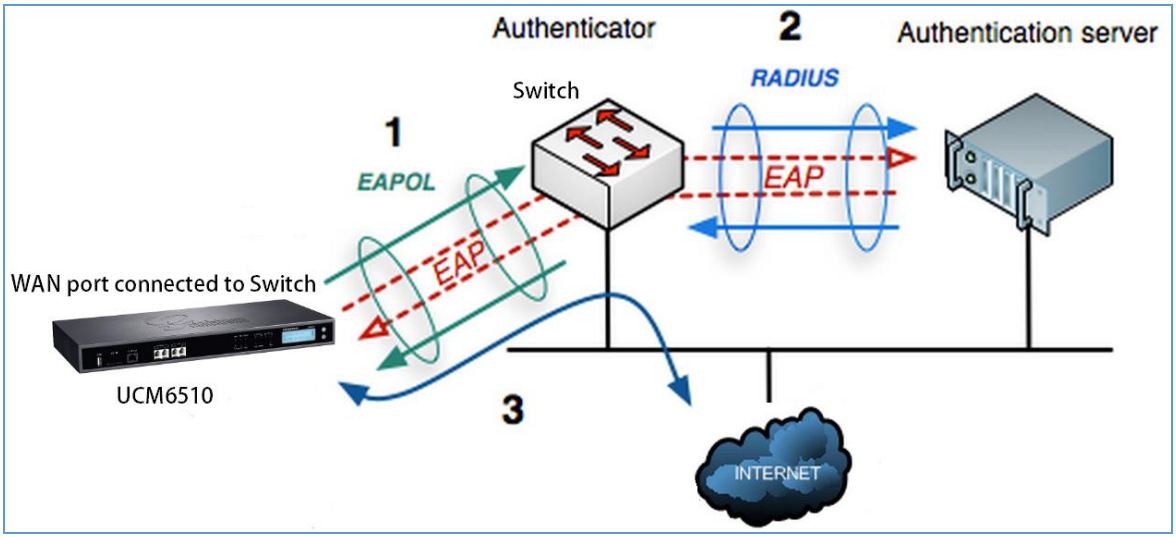


Figure 20: UCM6510 Using 802.1X as Client

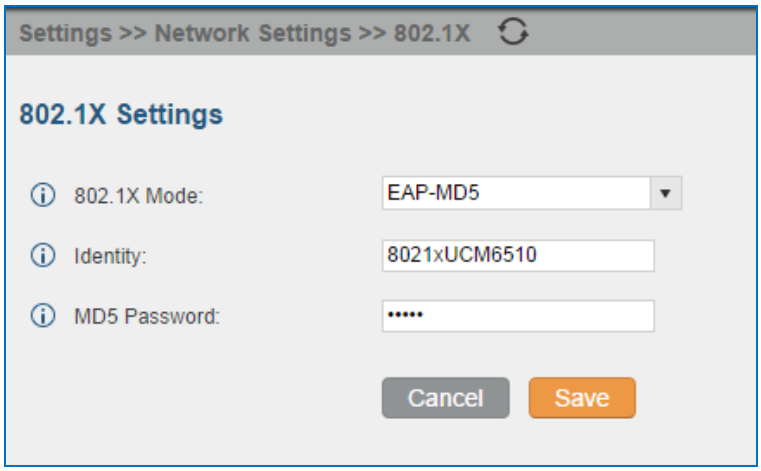


Figure 21: UCM6510 Using 802.1X EAP-MD5

The following table shows the configuration parameters for 802.1X on UCM6510. Identity and MD5 password are required for authentication, which should be provided by the network administrator obtained from the RADIUS server. If "EAP-TLS" or "EAP-PEAPv0/MSCHAPv2" is used as the 802.1X mode, users will also need upload 802.1X CA Certificate and 802.1X Client Certificate, which should be also generated from the RADIUS server.

Table 9: UCM6510 Network Settings->802.1X

802.1X Mode	Select 802.1X mode. The default setting is "Disable". The supported 802.1X mode are: • EAP-MD5 • EAP-TLS • EAP-PEAPv0/MSCHAPv2
Identity	Enter 802.1X mode identity information.
MD5 Password	Enter 802.1X mode MD5 password information.
802.1X CA Certificate	Select 802.1X certificate from local PC and then upload.
802.1X Client Certificate	Select 802.1X client certificate from local PC and then upload.

STATIC ROUTES

A static route is a pre-determined path that the network traffic travels to reach a specific host or network. On the UCM6510, the static route function allows the device to use manually configured routes, rather than dynamically assigned routes or default gateway configured in the UCM6510 web GUI->**Network Settings**->**Basic Settings** to forward traffic. It can be used to define a route when no other routes is

available or necessary, or used in complementary with existing routing on the UCM6510 as a failover backup, and etc.

- Click on Create New Static Route to create a new static route. The configuration parameters are listed in the table below.
- Once added, users can select to edit the static route.
- Select to delete the static route.
- Static routes configuration can be reset from LCD menu->Network Menu.

Table 10: UCM6510 Network Settings->Static Routes

Destination	Configure the destination IP address or the destination IP subnet for the UCM6510 to reach using the static route. Example: IP address – ***192.168.66.4*** IP subnet – ***192.168.66.0***
Netmask	Configure the subnet mask for the above destination address. If left blank, the default value is 255.255.255.255. Example: ***255.255.255.0***
Gateway	Configure the gateway address so that the UCM6510 can reach the destination via this gateway. Gateway address is optional. Example: ***192.168.40.5***
Interface	Specify the network interface “LAN”, “WAN” or “Data trunk 1” (“Data Trunk 1” option will show only when the data trunk is enabled) on the UCM6510 to reach the destination using the static route.

The following diagram shows a sample application of static route usage on UCM6510.

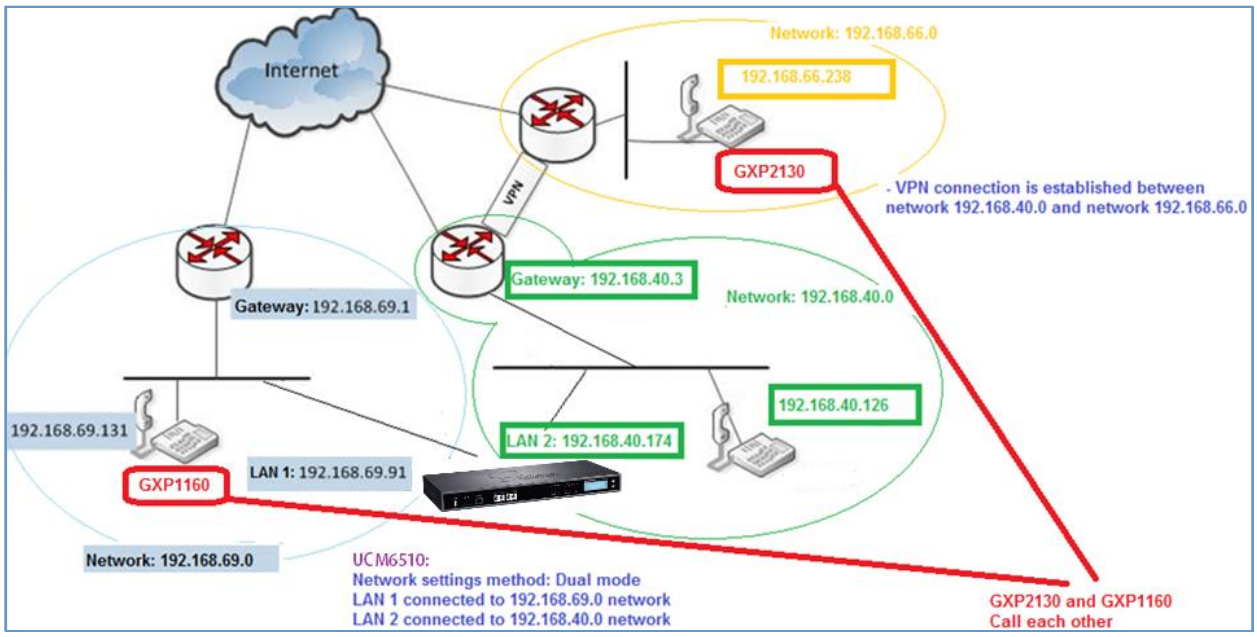


Figure 22: UCM6510 Static Route Sample

The network topology of the above diagram is as below:

- Network 192.168.69.0 has IP phones registered to UCM6510 LAN 1 address
- Network 192.168.40.0 has IP phones registered to UCM6510 LAN 2 address
- Network 192.168.66.0 has IP phones registered to UCM6510 via VPN
- Network 192.168.40.0 has VPN connection established with network 192.168.66.0

In this network, by default the IP phones in network 192.168.69.0 are unable to call IP phones in network 192.168.66.0 when registered on different interfaces on the UCM6510. Therefore, we need configure a static route on the UCM6510 so that the phones in isolated networks can make calls between each other.

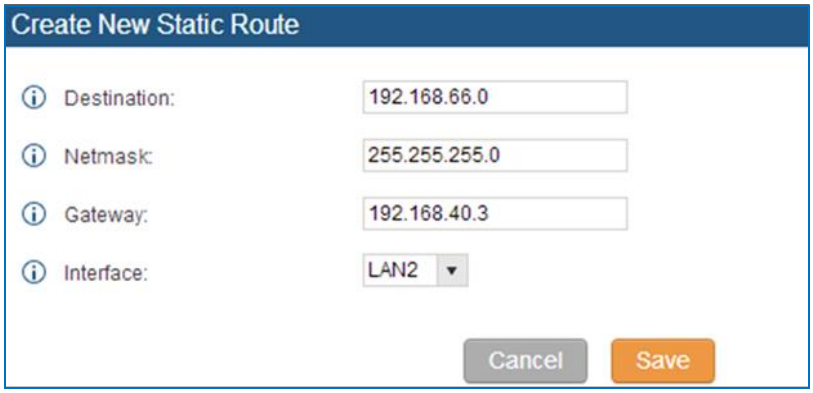


Figure 23: UCM6510 Static Route Configuration

PORT FORWORDING

The UCM6510 network interface supports router functions which provides users the ability to do port forwarding. If the UCM6510 is set to “Route” under web GUI->**Settings**->**Network Settings**->**Basic Settings: Method**, port forwarding is available for configuration.

The port forwarding configuration is under web GUI->**Settings**->**Network Settings**->**Port Forwarding** page. Please see related settings in the table below.

Table 11: UCM6510 Network Settings->Port Forwarding

WAN Port	Specify the WAN port number or a range of WAN ports. Up to 8 ports can be configured. **Note:** When it is set to a range, WAN port and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
LAN IP	Specify the LAN IP address.
LAN Port	Specify the LAN port number or a range of LAN ports. **Note:** When it is set to a range, WAN port and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
Protocol Type	Select protocol type “UDP Only”, “TCP Only” or “TCP/UDP” for the forwarding in the selected port. The default setting is “UDP Only”.

The following figures demonstrate a port forwarding example to provide phone’s web UI access to public side:

- The UCM6510 network mode is set to “Route”
- The UCM6510 WAN port is connected to uplink switch, with a public IP address configured, e.g. 1.1.1.1.
- The UCM6510 LAN port provides DHCP pool that connects to multiple phone devices in the LAN network 192.168.2.x. The UCM6510 is used as a router, with gateway address 192.168.2.1
- There is a GXP2160 connected under the LAN interface network of the UCM6510. It obtains IP address 192.168.2.100 from UCM6510 DHCP pool

- On the UCM6510 web UI->**Settings**->**Network Settings**->**Port Forwarding**, configure a port forwarding entry as the figure shows below.
  WAN Port: This is the port opened up on the WAN side for access purpose.
  LAN IP: This is the GXP2160 IP address, under the LAN interface network of the UCM6510.
  Protocol Type: We select TCP here for web UI access using HTTP.

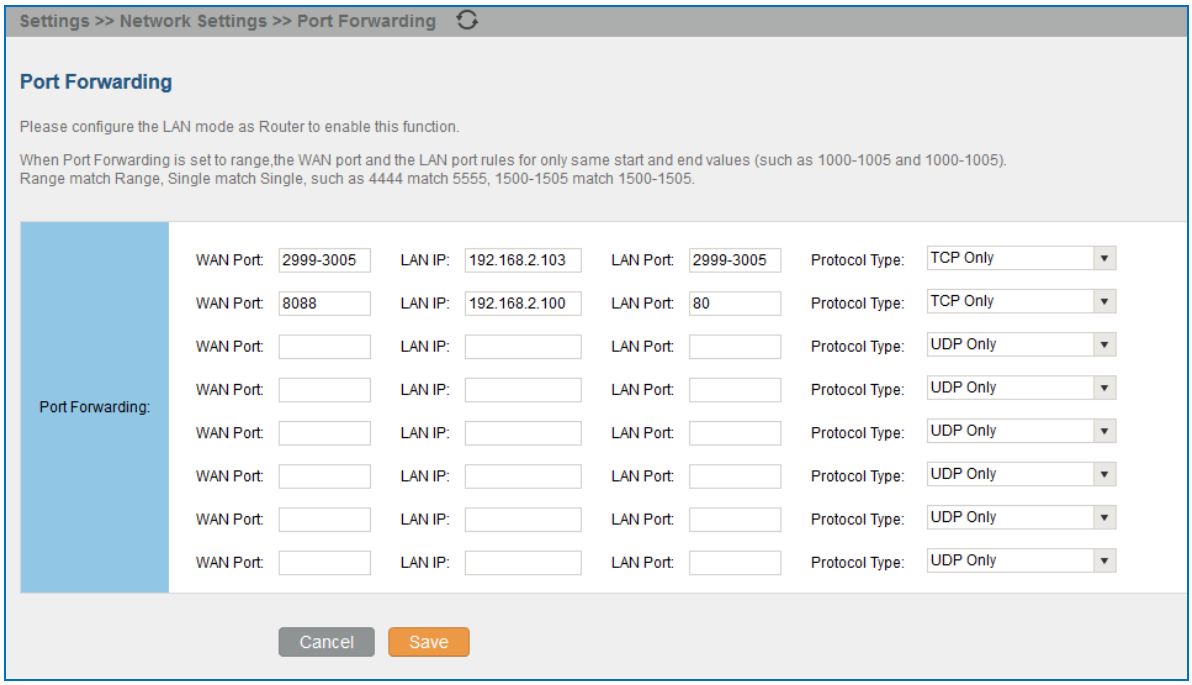

Settings >> Network Settings >> Port Forwarding
Port Forwarding
Please configure the LAN mode as Router to enable this function.
When Port Forwarding is set to range,the WAN port and the LAN port rules for only same start and end values (such as 1000-1005 and 1000-1005).
Range match Range, Single match Single, such as 4444 match 5555, 1500-1505 match 1500-1505.
Port Forwarding:
WAN Port: 2999-3005 LAN IP: 192.168.2.103 LAN Port: 2999-3005 Protocol Type: TCP Only
WAN Port: 8088 LAN IP: 192.168.2.100 LAN Port: 80 Protocol Type: TCP Only
WAN Port: LAN IP: LAN Port: Protocol Type: UDP Only
WAN Port: LAN IP: LAN Port: Protocol Type: UDP Only
WAN Port: LAN IP: LAN Port: Protocol Type: UDP Only
WAN Port: LAN IP: LAN Port: Protocol Type: UDP Only
WAN Port: LAN IP: LAN Port: Protocol Type: UDP Only
WAN Port: LAN IP: LAN Port: Protocol Type: UDP Only
Cancel
Save

Figure 24: UCM6510 Port Forwarding Configuration

This will allow users to access the GXP2160 web UI from public side, by typing in address “1.1.1.1:8088”.

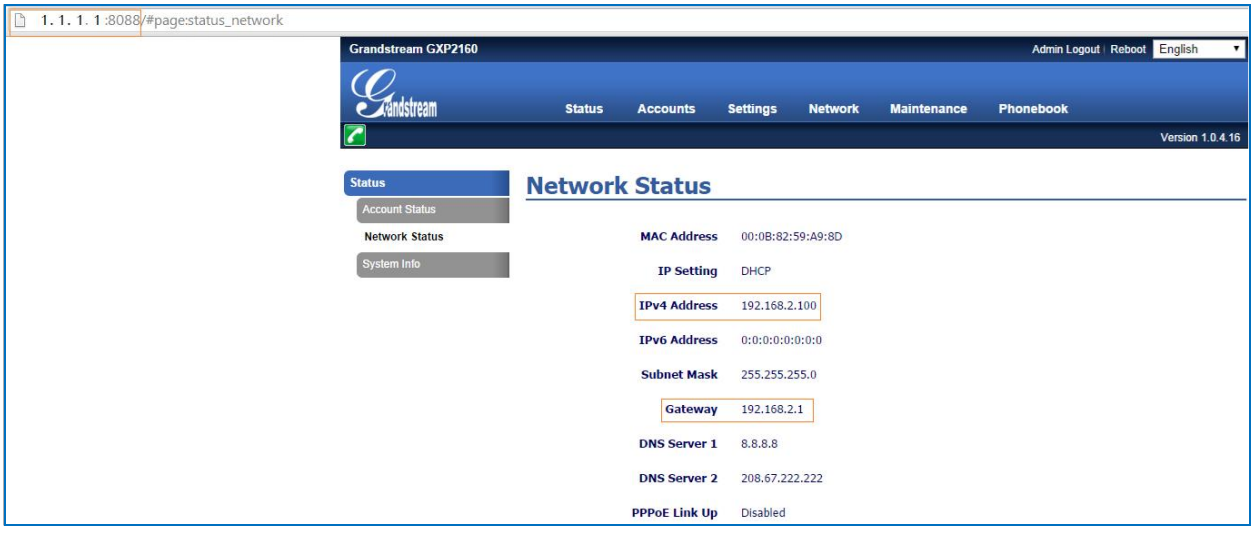


Figure 25: GXP2160 Web Access Using UCM6510 Port Forwarding

DDNS SETTINGS

DDNS setting allows user to access UCM6510 via domain name instead of IP address.
The UCM6510 supports DDNS service from the following DDNS provider:

- dydns.org
- noip.com
- freedns.afraid.org
- zoneedit.com
- oray.net

Here is an example of using noip.com for DDNS.

1. Register domain in DDNS service provider. Please note the UCM6510 needs to have public IP access.

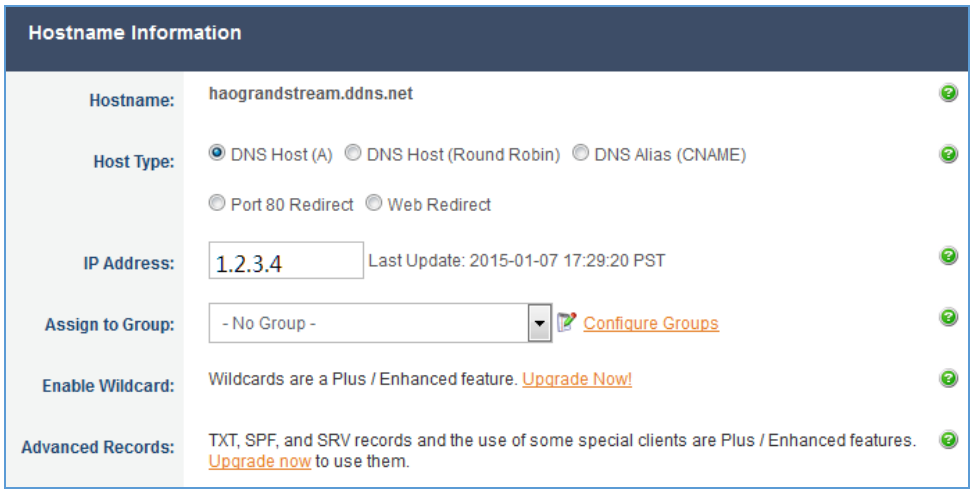


Figure 26: Register Domain Name on noip.com

2. On **web UI->Settings->Network Settings->DDNS Settings,** enable DDNS service and configure username, password and host name.

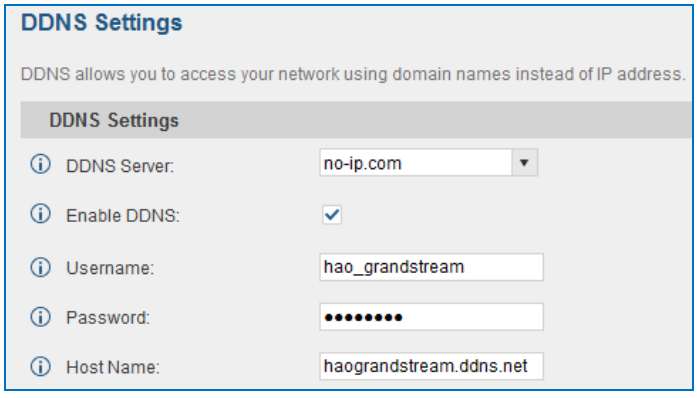


Figure 27: UCM6510 DDNS Setting

3. Now you can use domain name instead of IP address to connect to the UCM6510 web UI.

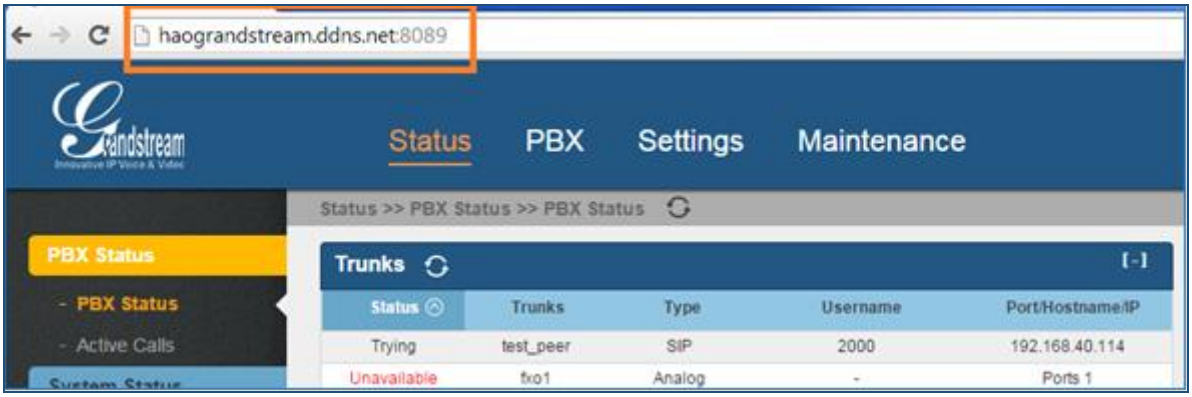


Figure 28: Using Domain Name to Connect to UCM6510

FIREWALL

The UCM6510 provides users firewall configurations to prevent certain malicious attack to the UCM6510 system. Users could configure to allow, restrict or reject specific traffic through the device for security and bandwidth purpose. The UCM6510 also provides Fail2ban feature for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE.

To configure firewall settings in UCM6510, go to web GUI->**Settings**->**Firewall** page.

STATIC DEFENSE

Under web GUI->**Settings**->**Firewall->Static Defense** page, users will see the following information:

- Current service information with port, process and type.
- Typical firewall settings.
- Custom firewall settings.

The following table shows a sample current service status running on the UCM6510.

Table 12: UCM6510 Firewall->Static Defense->Current Service

Port	Process	Type
7777	Asterisk	tcp/Ipv4
389	Slapd	tcp/Ipv4
22	Dropbear	tcp/Ipv4

80	Lighthttpd	tcp/Ipv4
8089	Lighthttpd	tcp/Ipv4
69	Opentftpd	udp/Ipv4
9090	Asterisk	udp/Ipv4
6060	zero_config	udp/Ipv4
5060	Asterisk	udp/Ipv4
4569	Asterisk	udp/Ipv4
5353	zero_config	udp/Ipv4
37435	Syslogd	udp/Ipv4

For typical firewall settings, users could configure the following options on the UCM6510.

Table 13: Typical Firewall Settings

Ping Defense Enable	If enabled, ICMP response will not be allowed for Ping request. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN interface.
Ping-of-Death Defense Enable	Enable to prevent Ping-of-Death attack to the device. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN interface.

Under “Custom Firewall Settings”, users could create new rules to accept, reject or drop certain traffic going through the UCM6510. To create new rule, click on “Create New Rule” button and a new window will pop up for users to specify rule options.

The following figure shows a firewall rule example that will deny SSH access for the UCM6510 from WAN side.

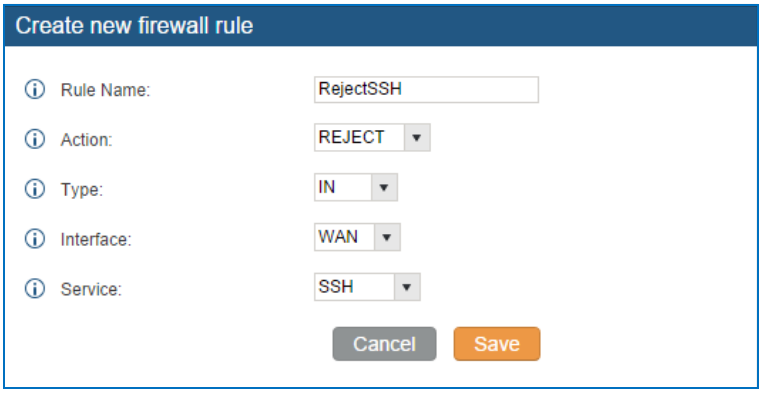


Figure 29: Create New Firewall Rule

Table 14: Firewall Rule Settings

Rule Name	Specify the Firewall rule name to identify the firewall rule.
Action	Select the action for the Firewall to perform. • ACCEPT • REJECT • DROP
Type	Select the traffic type. • IN If selected, users will need specify the network interface “LAN”, “WAN” or “Both” for the incoming traffic. • OUT
Service	Select the service type. • FTP • SSH • Telnet • TFTP • HTTP • LDAP • Custom If selected, users will need specify Source (IP and port), Destination (IP and port) and Protocol (TCP, UDP or Both) for the service. Please note if the source or the destination field is left blank, it will be used as “Anywhere”.

The new rule will be listed at the bottom of the page with sequence number, rule name, action, protocol, type, source, destination and operation. Users can click on to edit the rule, or click on to delete the rule. Save the change and reboot the device for the configuration to take effect.

DYNAMIC DEFENSE

Dynamic defense can blacklist hosts dynamically when the UCM6510 is set to “Route” under web GUI->**Settings**->**Network Settings**->**Basic Settings: Method**. If enabled, the traffic via TCP connection coming into the UCM6510 can be monitored, which helps prevent massive connection attempts or brute force attacks to the device. The blacklist can be created and updated by the UCM6510 firewall, which will then be displayed in the web page. Please refer to the following table for dynamic defense options on the UCM6510.

Table 15: UCM6510 Firewall Dynamic Defense

Dynamic Defense Enable	Enable dynamic defense. The default setting is disabled.
Periodical Time Interval	Configure the dynamic defense periodic time interval (in minutes). If the number of TCP connections from a host exceeds the “Connection Threshold” within this period, this host will be added into Blacklist. The valid value is between 1 and 59 when dynamic defense is turned on. The default setting is 59.
Blacklist Update Interval	Configure the blacklist update time interval (in seconds). The default setting is 120. This defines how long the IP will be blocked once added into the UCM6510 blacklist. For example, if it’s set to 300 seconds, the blocked IP address will only be able to establish TCP connection with the UCM6510 again after 300 seconds.
Connection Threshold	Configure the connection threshold. Once the number of connections from the same host reaches the threshold during “Periodical Time Interval”, it will be added into the blacklist. The default setting is 100.
Dynamic Defense Whitelist	Configure the dynamic defense whitelist. This is a list of Ips that will not be blocked by the UCM6510. For example, 192.168.1.3 192.168.1.4

The following figure shows a configuration example like this:

- If a host at IP address 192.168.40.7 initiates more than 20 TCP connections to the UCM6510 within 1 minute, it will be added into UCM6510 blacklist.
- This host 192.168.40.7 will be blocked by the UCM6510 for 300 seconds.
- Since IP address 192.168.40.5 is in whitelist, if the host at IP address 192.168.40.5 initiates more than 20 TCP connections to the UCM6510 within 1 minute, it will not be added into UCM6510 blacklist. It can still establish TCP connection with the UCM6510.

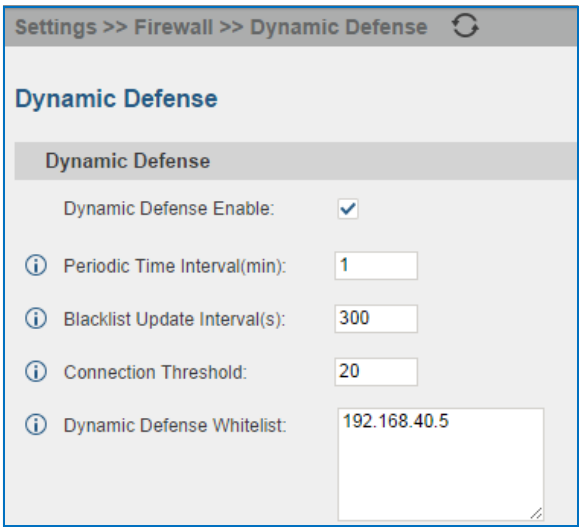


Figure 30: Configure Dynamic Defense

FAIL2BAN

Fail2Ban feature on the UCM6510 provides intrusion detection and prevention for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. Once the entry is detected within "Max Retry Duration", the UCM6510 will take action to forbid the host for certain period as defined in "Banned Duration". This feature helps prevent SIP brute force attacks to the PBX system.

Table 16: Fail2Ban Settings

Global Settings	
Enable Fail2Ban	Enable Fail2Ban. The default setting is disabled. Please make sure both "Enable Fail2Ban" and "Asterisk Service" are turned on in order to use Fail2Ban for SIP authentication on the UCM6510.
Banned Duration	Configure the duration (in seconds) for the detected host to be banned. The default setting is 300. If set to -1, the host will be always banned.
Max Retry Duration	Within this duration (in seconds), if a host exceeds the max times of retry as defined in "MaxRetry", the host will be banned. The default setting is 5.
MaxRetry	Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 10.
Fail2Ban Whitelist	Configure IP address, CIDR mask or DNS host in the whiltelist. Fail2Ban will not ban the host with matching address in this list. Up to 5 addresses can be added into the list.
Local Settings	
Asterisk Service	Enable Asterisk service for Fail2Ban. The default setting is disabled. Please make sure both "Enable Fail2Ban" and "Asterisk Service" are turned on in order to use

	Fail2Ban for SIP authentication on the UCM6510.
Protocol	Configure the listening port number for the service. Currently only 5060 (for UDP) is supported.
MaxRetry	Configure the number of authentication failures during “Max Retry Duration” before the host is banned. The default setting is 10. Please make sure this option is properly configured as it will override the “MaxRetry” value under “Global Settings”.

CHANGE PASSWORD

After logging in the web GUI for the first time, it is highly recommended for users to change the default password “admin” to a more complicated password for security purpose. Follow the steps below to change the web GUI access password.

1. Go to web GUI->**Settings**->**Change Password** page.
2. Enter the old password first.
3. Enter the new password and retype the new password to confirm. The new password has to be at least 4 characters. The maximum length of the password is 16 characters.
4. Click on “Save” and the user will be automatically logged out.
5. Once the web page comes back to the login page again, enter the username “admin” and the new password to login.

LDAP SERVER

The UCM6510 has an embedded LDAP server for users to manage corporate phonebook in a centralized manner.

- By default, the LDAP server has generated the first phonebook with **PBX DN** “ou=pbx,dc=pbx,dc=com” based on the UCM6510 user extensions already.
- Users could add new phonebook with a different **Phonebook DN** for other external contacts. For example, “ou=people,dc=pbx,dc=com”.
- All the phonebooks in the UCM6510 LDAP server have the same **Base DN** “dc=pbx,dc=com”.
- “cn” “ou” and “dc” are parts of LDAP data Interchange Format according to RFC 2849, which is how the LDAP tree is filtered.
  Cn= Common Name
  ou= Organization Unit
  dc= Domain Component
- Here is an example of how the search for “ou=pbx,dc=pbx,dc=com” is performed in LDAP server query.

From the dc=com Domain Component, find the dc=pbx Domain Component first. In the dc=pbx Domain Component, find the Organizational Unit called pbx (ou=pbx) and then find the object that has a Common Name of admin.

If users have the Grandstream phone provisioned by the UCM6510, the LDAP directory has been set up on the phone and can be used right away for users to access all phonebooks generated in the UCM6510.

Additionally, users could manually configure the LDAP client settings to manipulate the built-in LDAP server on the UCM6510. If the UCM6510 has multiple LDAP phonebooks created, in the LDAP client configuration, users could use “dc=pbx,dc=com” as Base DN to have access to all phonebooks on the UCM6510 LDAP server, or use a specific phonebook DN, for example “ou=people,dc=pbx,dc=com”, to access to phonebook with Phonebook DN “ou=people,dc=pbx,dc=com “ only.

To access LDAP Server settings, go to **web GUI**->**Settings**->**LDAP Server**.

LDAP SERVER CONFIGURATIONS

The following figure shows the default LDAP server configurations on the UCM6510.

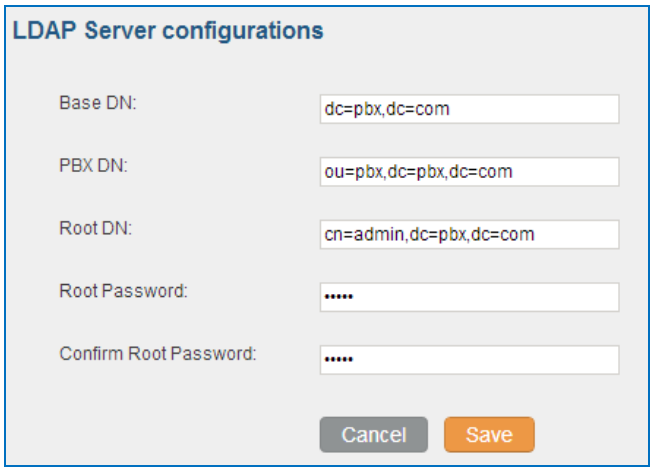


Figure 31: LDAP Server Configurations

The UCM6510 LDAP server supports anonymous access (read-only) by default. Therefore the LDAP client doesn’t have to configure username and password to access the phonebook directory. The “Root DN” and “Root Password” here are for LDAP management and configuration where users will need provide for authentication purpose before modifying the LDAP information.

The default phonebook list in this LDAP server can be viewed and edited by clicking on for the first phonebook under LDAP Phonebook.

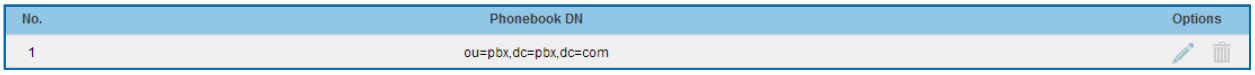


Figure 32: Default LDAP Phonebook DN

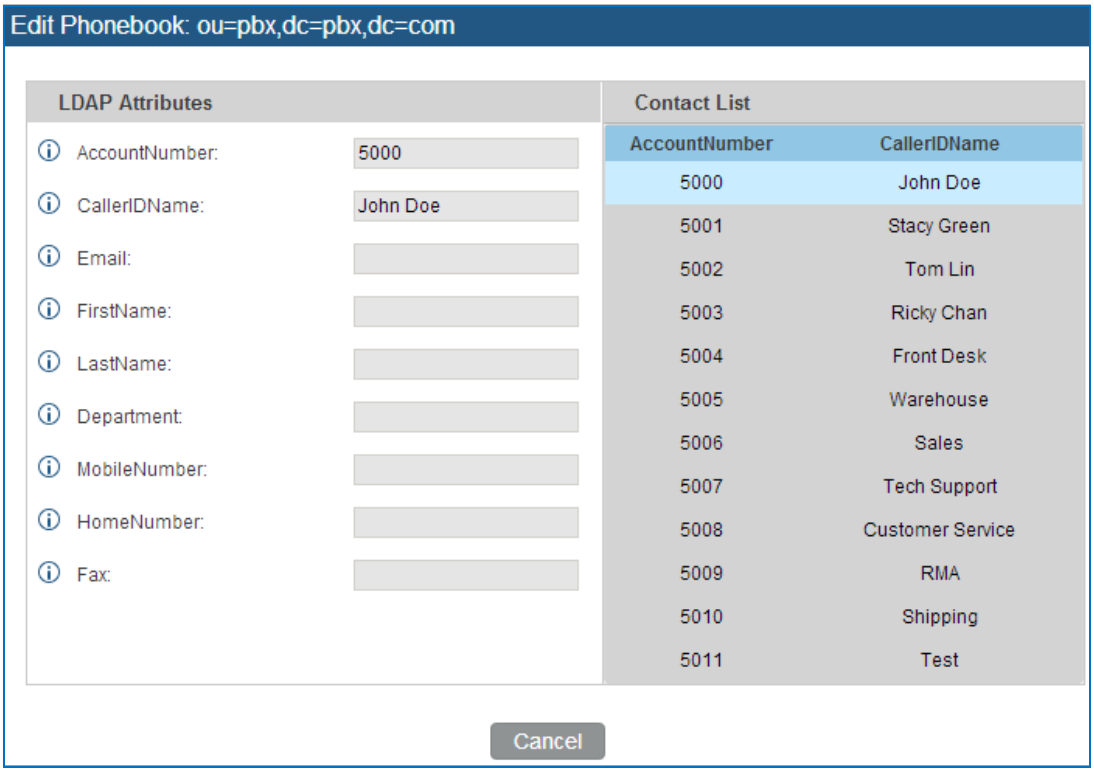


Figure 33: Default LDAP Phonebook Attributes

LDAP PHONEBOOK

Users could use the default phonebook, edit the default phonebook as well as add new phonebook on the LDAP server. The first phonebook with default phonebook dn "ou=pbx,dc=pbx,dc=com" displayed on the LDAP server page is for extensions in this PBX. Users cannot add or delete contacts directly. The contacts information will need to be modified via web GUI->**PBX**->**Basic/Call Routes**->**Extensions** first. The default LDAP phonebook will then be updated automatically.

- **Add new phonebook**

  A new sibling phonebook of the default PBX phonebook can be added by clicking on "Add" under "LDAP Phonebook" section.

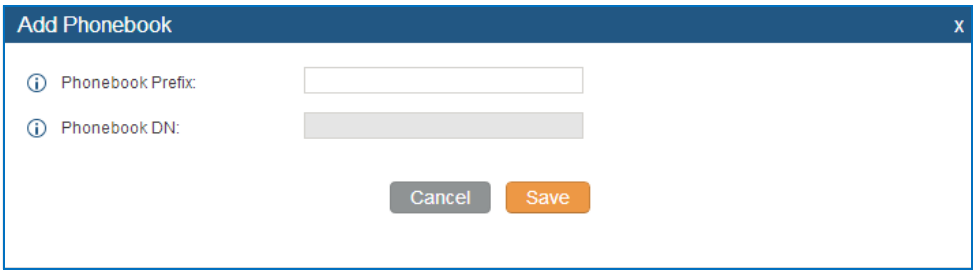


Figure 34: Add LDAP Phonebook

Configure the “Phonebook Prefix” first. The “Phonebook DN” will be automatically filled in. For example, if configuring “Phonebook Prefix” as “people”, the “Phonebook DN” will be filled with “ou=people,dc=pbx,dc=com”.

Once added, users can select to edit the phonebook attributes and contact list (see figure below), or select to delete the phonebook.

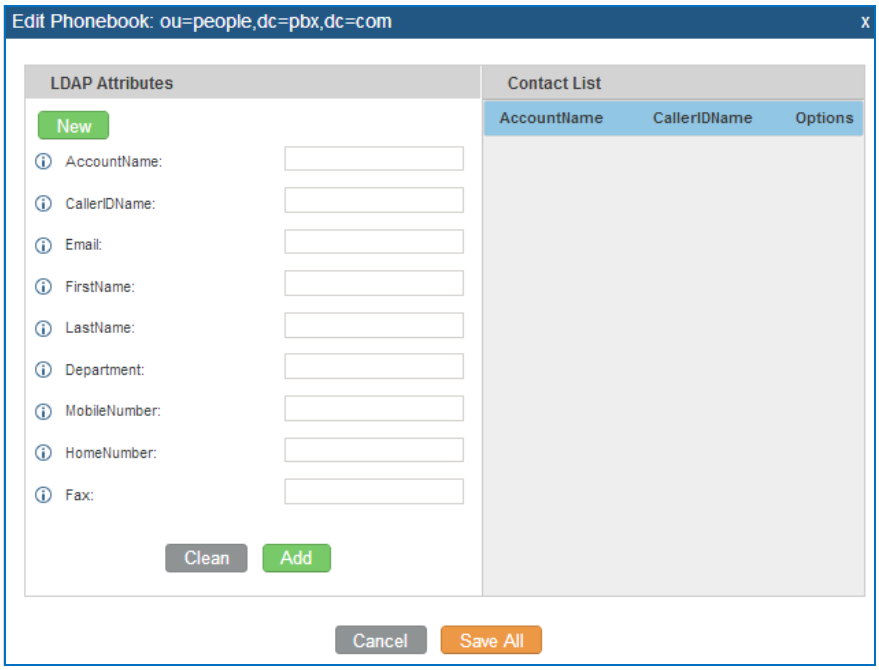


Figure 35: Edit LDAP Phonebook

- **Import phonebook from your computer to LDAP server**

  Click on “Import Phonebook” and a dialog will prompt as shown in the figure below.

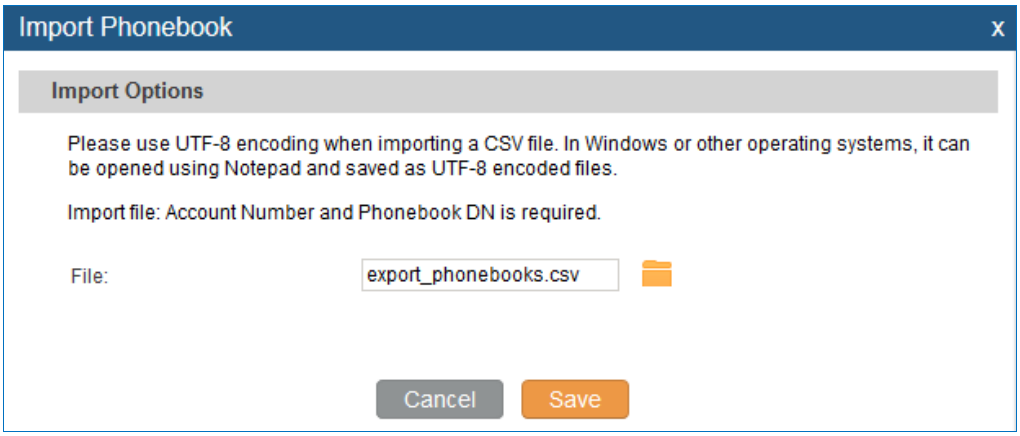

Import Phonebook
x
Import Options
Please use UTF-8 encoding when importing a CSV file. In Windows or other operating systems, it can be opened using Notepad and saved as UTF-8 encoded files.
Import file: Account Number and Phonebook DN is required.
File:
export_phonebooks.csv
Cancel
Save

Figure 36: Import Phonebook

The file to be imported must be a CSV file with UTF-8 encoding. Users can open the CSV file with Notepad and save it with UTF-8 encoding.

Here is how a sample file looks like. Please note “Account Number” and “Phonebook DN” fields are required. Users could export a phonebook file from the UCM6510 LDAP phonebook section first and use it as a sample to start with.

	A	B	C	D	E	F	G	H	I	J
1	First Nam	Last Name	Account Number	CallerID Name	Email	Department	Mobile Number	Home Number	Fax	Phonebook DN
2	John	Doe	1001	1001		IT	1001000000			phonebook
3	Jane	Doe	1002	1002		Sales	1002000000			phonebook
4	William	Chung	1003	1003		Marketing	1003000000			phonebook
5	Linda	Kuo	1004	1004		Accounting	1004000000			phonebook
6	Steve	Chang	1005	1005		Support	1005000000			others

Figure 37: Phonebook CSV File Format

The Phonebook DN field is the same “Phonebook Prefix” entry as when the user clicks on “Add” to create a new phonebook. Therefore, if the user enters “phonebook” in “Phonebook DN” field in the CSV file, the actual phonebook DN “ou=phonebook,dc=pbx,dc=com” will be automatically created by the UCM6510 once the CSV file is imported.

In the CSV file, users can specify different phonebook DN fields for different contacts. If the phonebook DN already exists on the UCM6510 LDAP Phonebook, the contacts in the CSV file will be added into the existing phonebook. If the phonebook DN doesn’t exist on the UCM6510 LDAP Phonebook, a new phonebook with this phonebook DN will be created.

The sample phonebook CSV file in above picture will result in the following LDAP phonebook in the UCM6510.

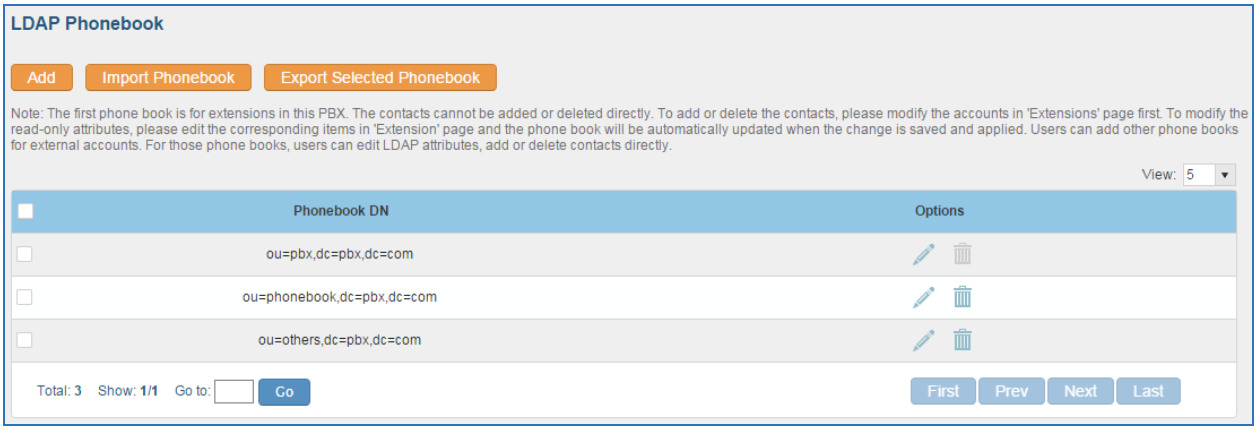

LDAP Phonebook
Add
Import Phonebook
Export Selected Phonebook
Note: The first phone book is for extensions in this PBX. The contacts cannot be added or deleted directly. To add or delete the contacts, please modify the accounts in 'Extensions' page first. To modify the read-only attributes, please edit the corresponding items in 'Extension' page and the phone book will be automatically updated when the change is saved and applied. Users can add other phone books for external accounts. For those phone books, users can edit LDAP attributes, add or delete contacts directly.
View: 5
Phonebook DN
Options
ou=pbx,dc=pbx,dc=com
ou=phonebook,dc=pbx,dc=com
ou=others,dc=pbx,dc=com
Total: 3 Show: 1/1 Go to: Go
First Prev Next Last

Figure 38: LDAP Phonebook After Import

As the default LDAP phonebook with DN “ou=pbx,dc=pbx,dc=com” cannot be edited or deleted in LDAP phonebook section, users cannot import contacts with Phonebook DN field “pbx” if existed in the CSV file.

- **Export phonebook to your computer from UCM6510 LDAP server**

  Select the checkbox for the LDAP phonebook and then click on “Export Selected Phonebook” to export the selected phonebook. The exported phonebook can be used as a record or a sample CSV file for the users to add more contacts in it and import to the UCM6510 again.

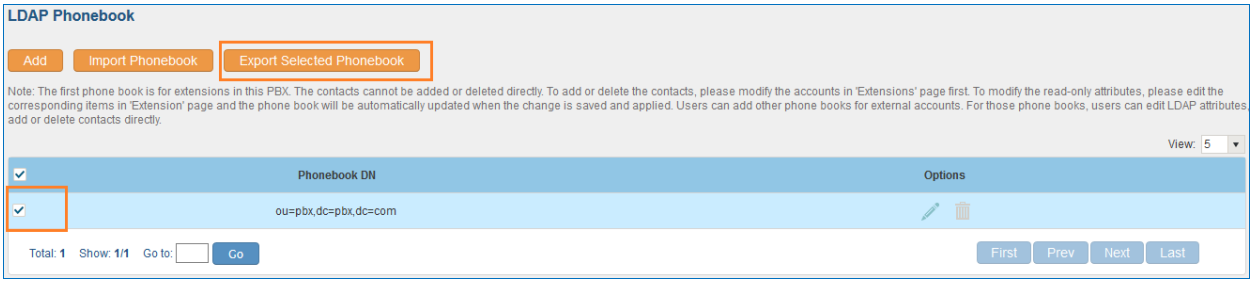

LDAP Phonebook
Add
Import Phonebook
Export Selected Phonebook
Note: The first phone book is for extensions in this PBX. The contacts cannot be added or deleted directly. To add or delete the contacts, please modify the accounts in 'Extensions' page first. To modify the read-only attributes, please edit the corresponding items in 'Extension' page and the phone book will be automatically updated when the change is saved and applied. Users can add other phone books for external accounts. For those phone books, users can edit LDAP attributes, add or delete contacts directly.
View: 5
Phonebook DN
Options
ou=pbx,dc=pbx,dc=com
Total: 1 Show: 1/1 Go to: Go
First Prev Next Last

Figure 39: Export Selected LDAP Phonebook

LDAP CLIENT CONFIGURATIONS

The configuration on LDAP client is similar when you use other LDAP servers. Here we provide an example on how to configure the LDAP client on the SIP end points to use the default PBX phonebook.

Assuming the server base dn is “dc=pbx,dc=com”, configure the LDAP clients as follows (case insensitive):

Base DN: dc=pbx,dc=com
Login DN: Please leave this field empty
Password: Please leave this field empty
Anonymous: Please enable this option
Filter: (|(CallerIDName=%)(AccountNumber=%))
Port: 389

The following figure gives a sample configurations for UCM6510 acting as a LDAP client.

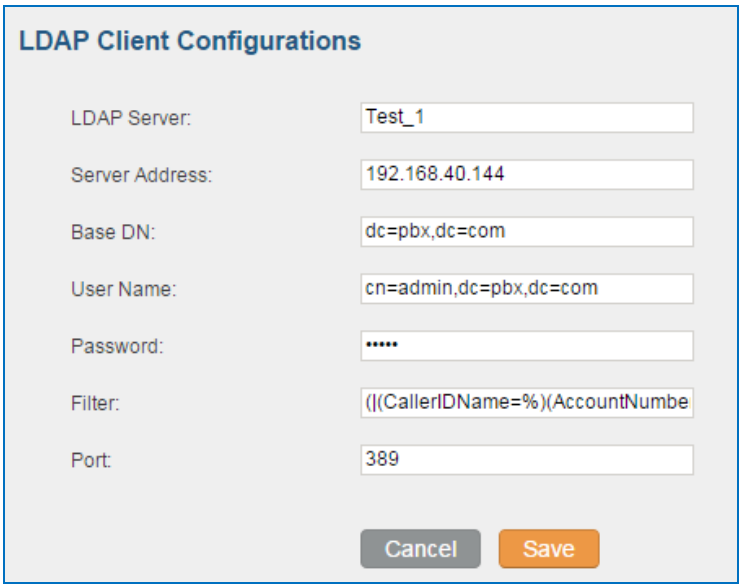


Figure 40: LDAP Client Configurations

To configure Grandstream IP phones as the LDAP client, please refer to the following example:

Server Address: The IP address or domain name of the UCM6510
Base DN: dc=pbx,dc=com
User Name: Please leave this field empty
Password: Please leave this field empty
LDAP Name Attribute: CallerIDName Email Department FirstName LastName
LDAP Number Attribute: AccountNumber MobileNumber HomeNumber Fax
LDAP Number Filter: (AccountNumber=%)
LDAP Name Filter: (CallerIDName=%)
LDAP Display Name: AccountNumber CallerIDName
LDAP Version: If existed, please select LDAP Version 3
Port: 389

The following figure shows the configuration information on a Grandstream GXP2200 to successfully use the LDAP server as configured in ***[Figure 31: LDAP Server Configurations]***.

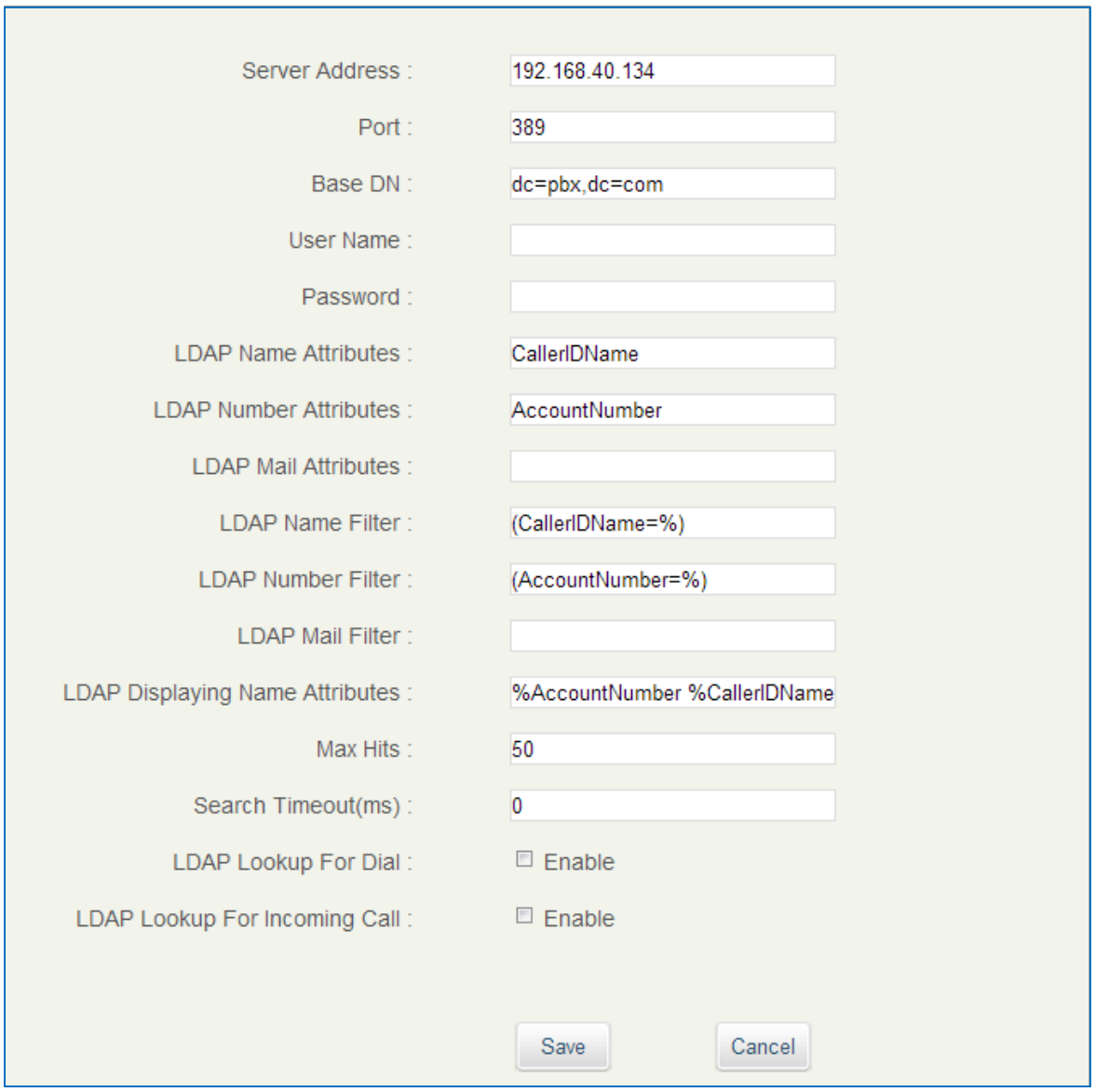


Figure 41: GXP2200 LDAP Phonebook Configuration

HTTP SERVER

The UCM6510 embedded web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow the users to configure the PBX through a web browser such as Microsoft IE, Mozilla Firefox and Google Chrome. By default, the PBX can be accessed directly by typing IP address in the PC's web browser (e.g., 192.168.40.50). It will then be automatically redirected to HTTPS using Port 8089 (e.g., https://192.168.40.50:8089). Users could also change the access protocol and port as preferred under web GUI->**Settings**->**HTTP Server**.

Table 17: HTTP Server Settings

Redirect From Port 80	Enable or disable redirect from port 80. On the PBX, the default access protocol is HTTPS and the default port number is 8089. When this option is enabled, the access using HTTP with Port 80 will be redirected to HTTPS with Port 8089. The default setting is “Enable”.
Protocol Type	Select HTTP or HTTPS as the protocol to access the HTTP server. The default setting is “HTTPS”. This also defines whether to use HTTP or HTTPS to download the config file in zero config as the UCM6510 is served as HTTP/HTTPS server that has the device config files for zero config.
Port	Specify port number to access the HTTP server. The default port number is 8089.

Once the change is saved, the web page will be redirected to the login page using the new URL. Enter the username and password to login again.

EMAIL SETTINGS

The Email application on the UCM6510 can be used to send out alert event Emails, Fax (Fax-To-Email), Voicemail (Voicemail-To-Email) and etc. The configuration parameters can be accessed via web GUI->**Settings**->**Email Settings**.

Table 18: Email Settings

TLS Enable	Enable or disable TLS during transferring/submitting your Email to other SMTP server. The default setting is “Yes”.
Type	• MTA: Mail Transfer Agent. The Email will be sent from the configured domain. When MTA is selected, there is no need to set up SMTP server for it or no user login is required. However, the Emails sent from MTA might be considered as spam by the target SMTP server. • Client: Submit Emails to the SMTP server. A SMTP server is required and users need login with correct credentials.
Domain	Specify the domain name to be used in the Email when using type “MTA”.
Server	Specify the SMTP server when using type “Client”. For example, if using Gmail as the SMTP server, you can configure it as *smtp.gmail.com:465.*
Username	Username is required when using type “Client”. Normally it’s the Email address.
Password	Password to log in for the above Username (Email address) is required when using type “Client”.
Display Name	Specify the display name in the FROM header in the Email.

Sender	Specify the sender's Email address. For example, pbx@example.mycompany.com.

The following figure shows a sample Email settings on the UCM6510, assuming the Email is using *smtp.gmail.com* as the SMTP server and the port number is 465.

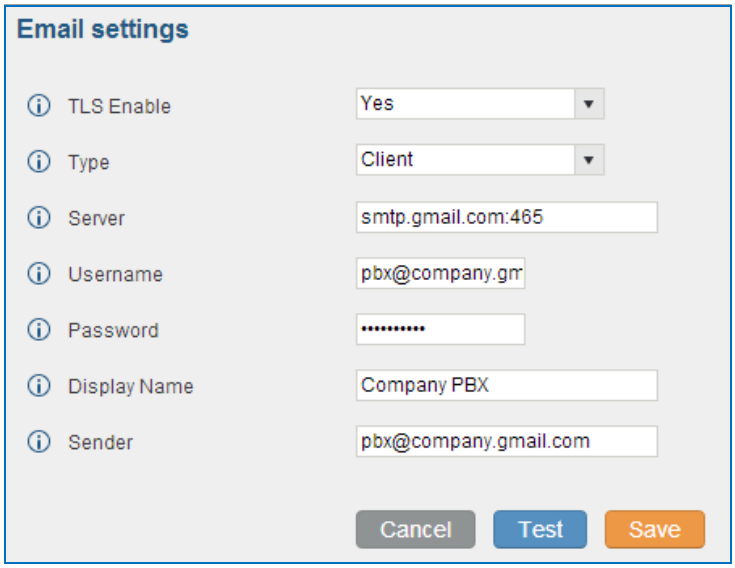


Figure 42: UCM6510 Email Settings

Once the configuration is finished, click on "Save" first. Then click on "Test" button to make sure the Email setting is working.

The following figure shows the new dialog prompted to test the Email setting. Fill in a valid Email address to send a test Email to verify the Email settings on the UCM6510.

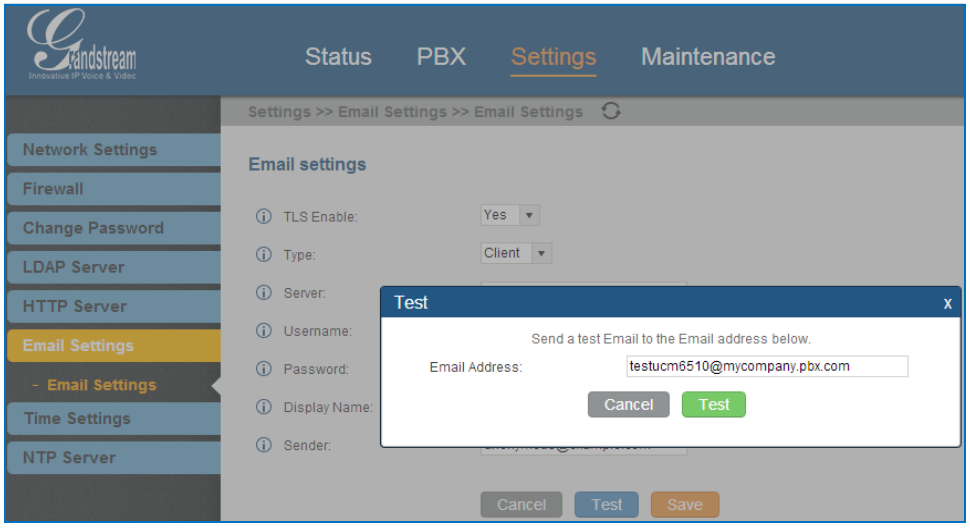


Figure 43: UCM6510 Email Settings: Send Test Email

TIME SETTINGS

AUTO TIME UPDATING

The current system time on the UCM6510 is displayed on the upper right of the web page. It can also be found under web GUI->**Status**->**System Status**->**General**.

To configure the UCM6510 to update time automatically, go to web GUI->**Settings**->**Time Settings**-> **Auto Time Updating**.

Note:

The configurations under Web GUI->**Settings**->**Time Settings**->**Time Auto Updating** page require reboot to take effect. Please consider configuring auto time updating related changes when setting up the UCM6510 for the first time to avoid service interrupt after installation and deployment in production.

Table 19: Auto Time Updating

Remote NTP Server	Specify the URL or IP address of the NTP server for the UCM6510 to synchronize the date and time. The default NTP server is ntp.ipvideotalk.com.
Enable DHCP Option 2	If set to “Yes”, the UCM6510 is allowed to get provisioned for Time Zone from DHCP Option 2 in the local server automatically. The default setting is “Yes”.
Enable DHCP Option 42	If set to “Yes”, the UCM6510 is allowed to get provisioned for NTP Server from DHCP Option 42 in the local server automatically. This will override the manually configured NTP Server. The default setting is “Yes”.
Time Zone	Select the proper time zone option so the UCM6510 can display correct time accordingly. If “Self-Defined Tome Zone” is selected, please specify the time zone parameters in “Self-Defined Time Zone” field as described in below option.

Self-Defined Time Zone	If “Self-Defined Time Zone” is selected in “Time Zone” option, users will need define their own time zone following the format below. The syntax is: std offset dst [offset], start [/time], end [/time] Default is set to: MTZ+6MDT+5,M4.1.0,M11.1.0 **MTZ+6MDT+5** This indicates a time zone with 6 hours offset and 1 hour ahead for DST, which is U.S central time. If it is positive (+), the local time zone is west of the Prime Meridian (A.K.A: International or Greenwich Meridian); If it is negative (-), the local time zone is east. **M4.1.0,M11.1.0** The 1st number indicates Month: 1, 2, 3…, 12 (for Jan, Feb…Dec.). The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday…). Normally 1, 2, 3, 4 are used. If 5 is used, it means the last iteration of the weekday. The 3rd number indicates weekday: 0, 1, 2…6 (for Sun, Mon, Tues… Sat). Therefore, this example is the DST which starts from the First Sunday of April to the 1st Sunday of November.

SET TIME MANUALLY

To manually set the time on the UCM6510, go to Web GUI->**Settings**->**Time Settings**->**Set Time Manually**. The format is YYYY-MM-DD HH:MI:SS.

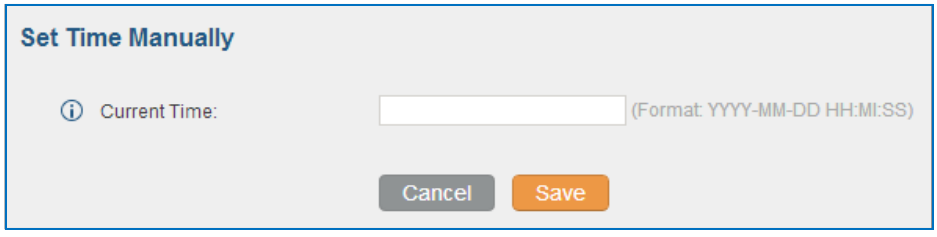


Figure 44: Set Time Manually

Note:

Manually setup time will take effect immediately after saving and applying change in the web UI. If users would like to reboot the UCM6510 and keep the manually setup time setting, please make sure “Remote NTP Server”, “Enable DHCP Option 2” and “Enable DHCP Option 42” options under Web GUI->**Settings**->**Time Settings**->**Time Auto Updating** page are unchecked or set to empty. Otherwise, time auto updating settings in this page will take effect after reboot.

OFFICE TIME

On the UCM6510, the system administrator can define “office time”, which can be used to configure time condition for extension call forwarding schedule and inbound rule schedule. To configure office time, go to Web GUI->**Settings**->**Time Settings**->**Office Time**. Click on “Create New Office Time” to create an office time.

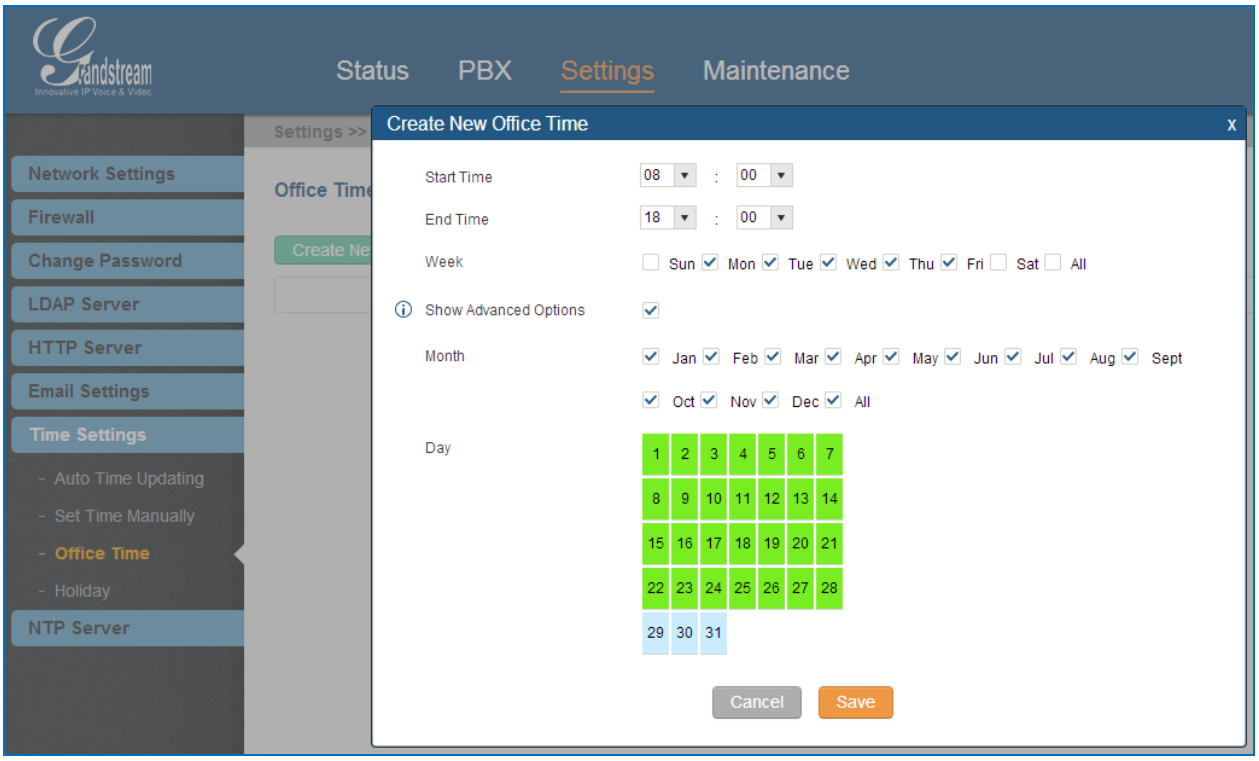


Figure 45: Create New Office Time

Table 20: Create New Office Time

Start Time	Configure the start time for office hour.
End Time	Configure the end time for office hour
Week	Select the work days in one week.
Show Advanced Options	Check this options to show advanced options. Once selected, please specify “Month” and “Day” below.
Month	Select the months for office time.
Day	Select the work days in one month.

Select “Start Time”, “End Time” and the day for the “Week” for the office time. The system administrator can also define month and day of the month as advanced options. Once done, click on “Save” and then “Apply Change” for the office time to take effect. The office time will be listed in the web page as the figure shows below.

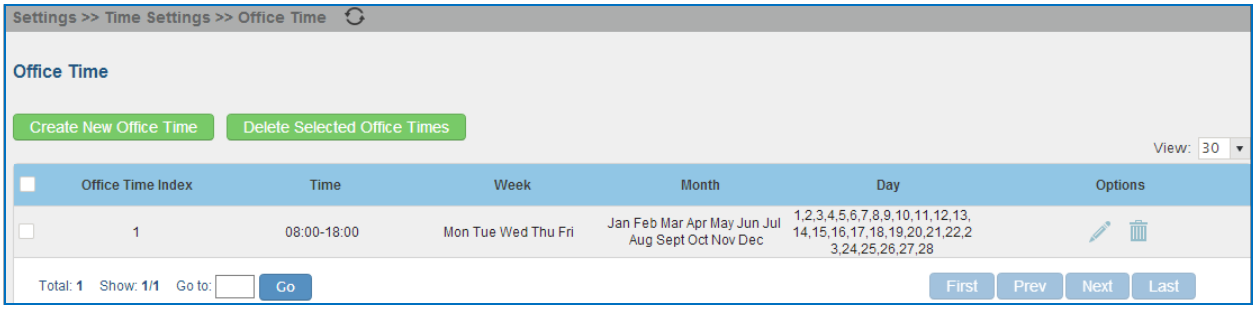


Figure 46: Settings->Time Settings->Office Time

- Click on to edit the office time.
- Click on to delete the office time.
- Click on “Delete Selected Office Times” to delete multiple selected office times at once.

HOLIDAY

On the UCM6510, the system administrator can define “holiday”, which can be used to configure time condition for extension call forwarding schedule and inbound rule schedule. To configure holiday, go to Web GUI->**Settings**->**Time Settings**->**Holiday**. Click on “Create New Holiday” to create holiday time.

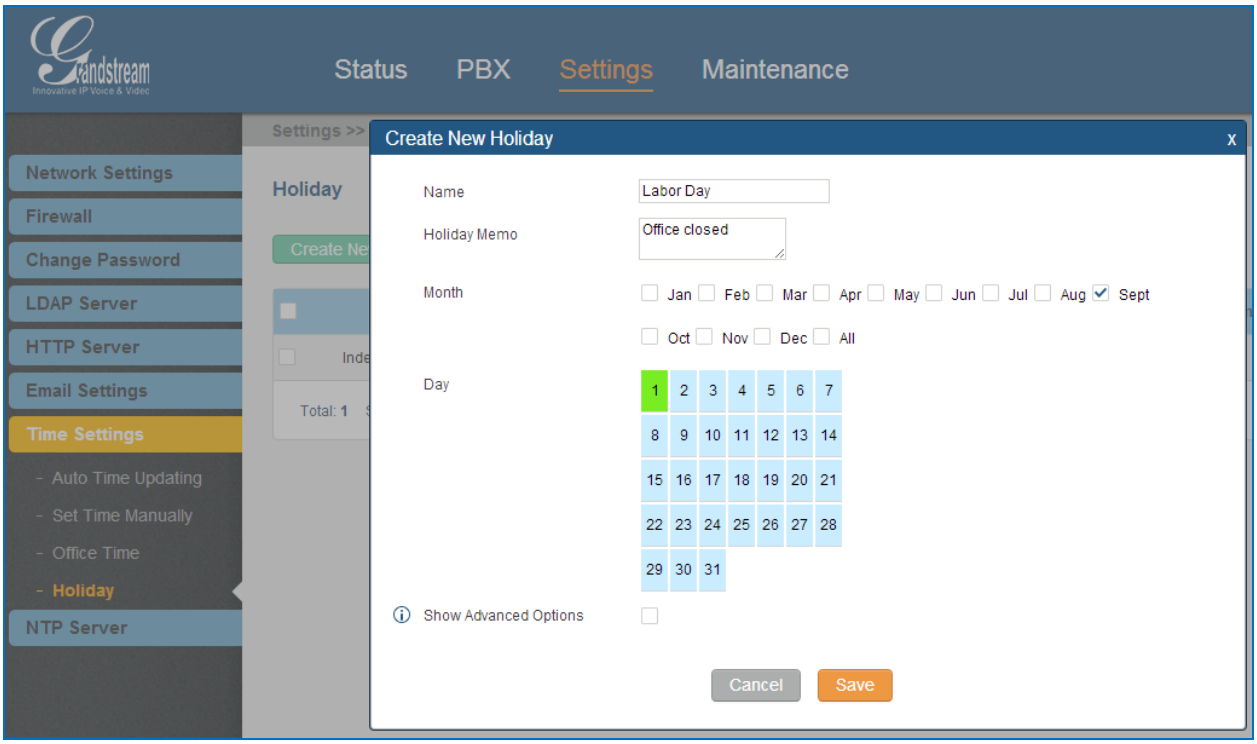


Figure 47: Create New Holiday

Table 21: Create New Holiday

Name	Specify the holiday name to identify this holiday.
Holiday Memo	Create a note for the holiday.
Month	Select the month for the holiday.
Day	Select the day for the holiday.
Show Advanced Options	Check this option to show advanced options. If selected, please specify the days as holiday in one week below.
Week	Select the days as holiday in one week.

Enter holiday “Name” and “Holiday Memo” for the new holiday. Then select “Month” and “Day”. The system administrator can also define days in one week as advanced options. Once done, click on “Save” and then “Apply Change” for the holiday to take effect. The holiday will be listed in the web page as the figure shows below.

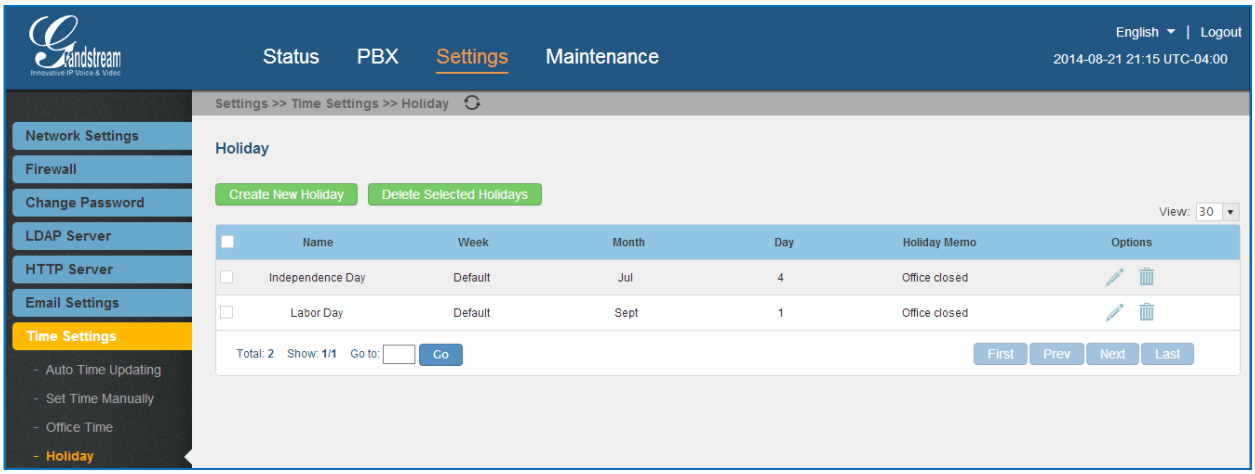


Figure 48: Settings->Time Settings->Holiday

- Click on to edit the holiday.
- Click on to delete the holiday.
- Click on "Delete Selected Holidays" to delete multiple selected holidays at once.

Note:

For more details on how to use office time and holiday, please refer to the link below: http://www.grandstream.com/products/ucm_series/ucm61xx/documents/how_to_use_office_time_and_holiday_ucm6100.pdf

---

NTP SERVER

The UCM6510 can be used as a NTP server for the NTP clients to synchronize their time with. To configure the UCM6510 as the NTP server, set "Enable NTP server" to "Yes" under web GUI->**Settings**->**Time Settings**->**NTP Server**. On the client side, point the NTP server address to the UCM6510 IP address or host name to use the UCM6510 as the NTP server.

RECORDINGS STORAGE

The UCM6510 supports call recordings automatically or manually and the recording files can be saved in external storage plugged in the UCM6510 or on the UCM6510 locally. To manage the recording storage, users can go to UCM6510 web GUI->**Settings**->**Recordings Storage** page and select whether to store the recording files in USB Disk, SD card or locally on the UCM6510.

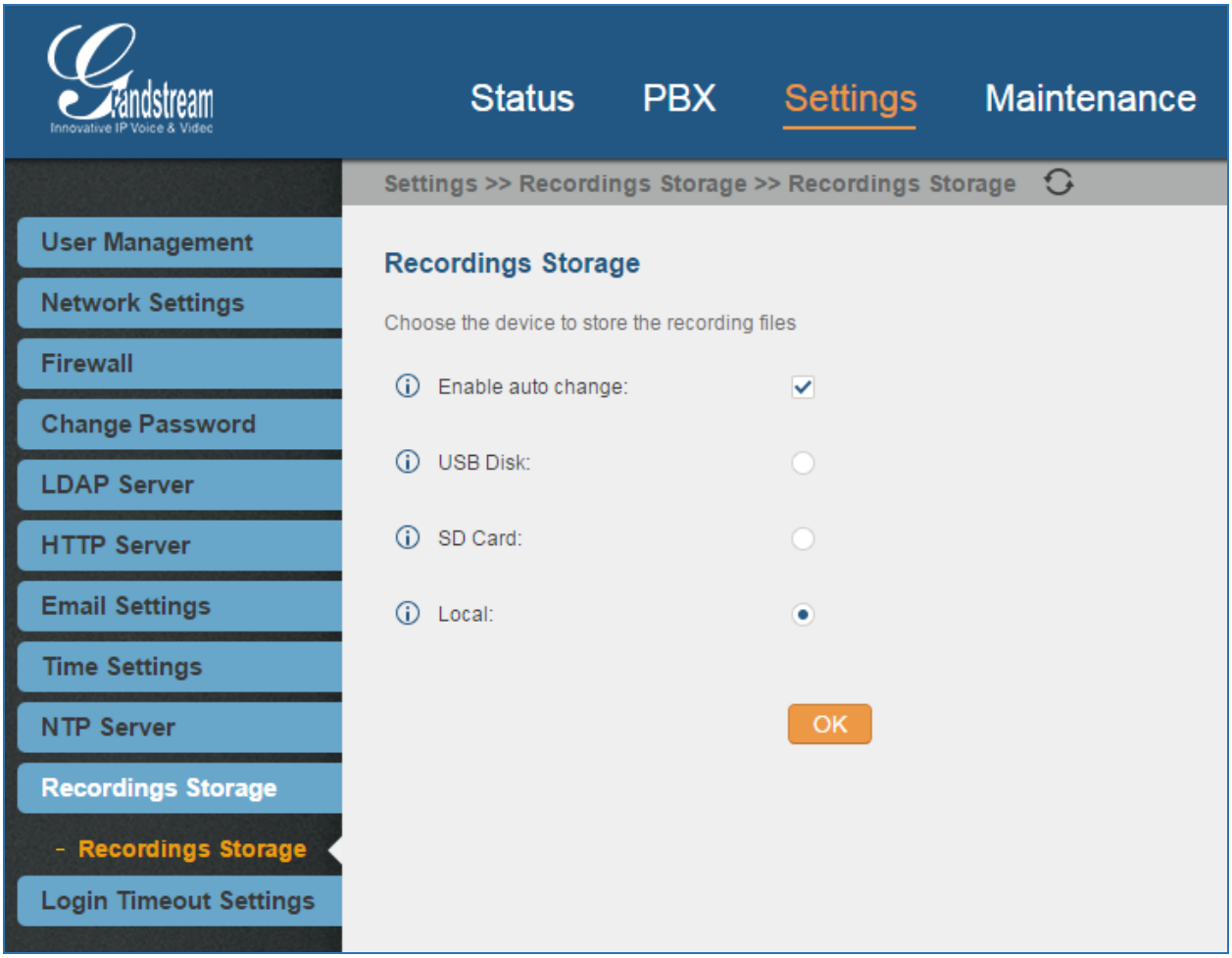


Figure 49: Settings->Recordings Storage

- If “Enable Auto Change” is selected, the recording files will be automatically saved in the available USB Disk or SD card plugged into the UCM6510. If both USB Disk and SD card are plugged in, the recording files will be always saved in the USB Disk.

- If “Local” is selected, the recordings will be stored in UCM6510 internal storage.

- If “USB Disk” or “SD Card” is selected, the recordings will be stored in the corresponding plugged in external storage device. Please note the options “USB Disk” and “SD Card” will be displayed only if they are plugged into the UCM6510.

  Once “USB Disk” or “SD Card” is selected, click on “OK”. The user will be prompted to confirm to copy the local files to the external storage device.

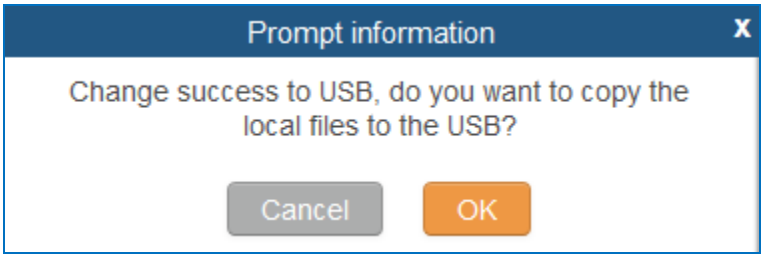


Figure 50: Recordings Storage Prompt Information

  Click on “OK” to continue. The users will be prompted a new dialog to select the categories for the files to be copied over.

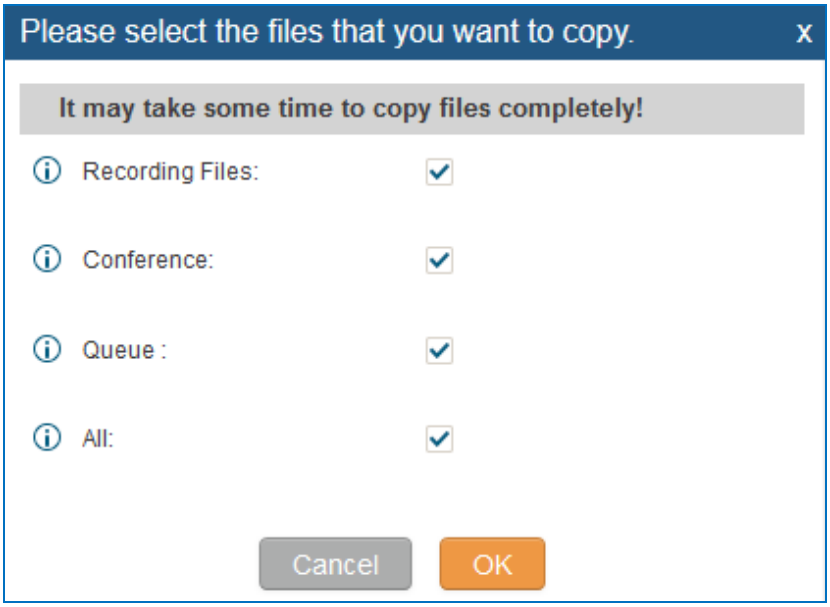


Figure 51: Recording Storage Category

  On the UCM6510, recording files are generated and exist in 3 categories: normal call recording files, conference recording files, and call queue recording files. Therefore users have the following options when select the categories to copy the files to the external device:

  - Recording Files: Copy the normal recording files to the external device.
  - Conference: Copy the conference recording files to the external device.
  - Queue: Copy the call queue recording files to the external device.

- All: Copy all recording files to the external device.

LOGIN TIMEOUT SETTINGS

After the user logs in the UCM6510 web UI, the user will be automatically logged out after certain timeout. This timeout value can be specified under UCM6510 web GUI->**Settings**->**Login Timeout Settings** page.

The "User Login Timeout" value is in minute and the default setting is 10 minutes. If the user doesn't make any operation on web UI within the timeout, the user will be logged out automatically. After that, the web UI will be redirected to the login page and the user will need to enter username and password to log in.

If set to 0, there is no timeout for the web UI login session and the user will not be automatically logged out.

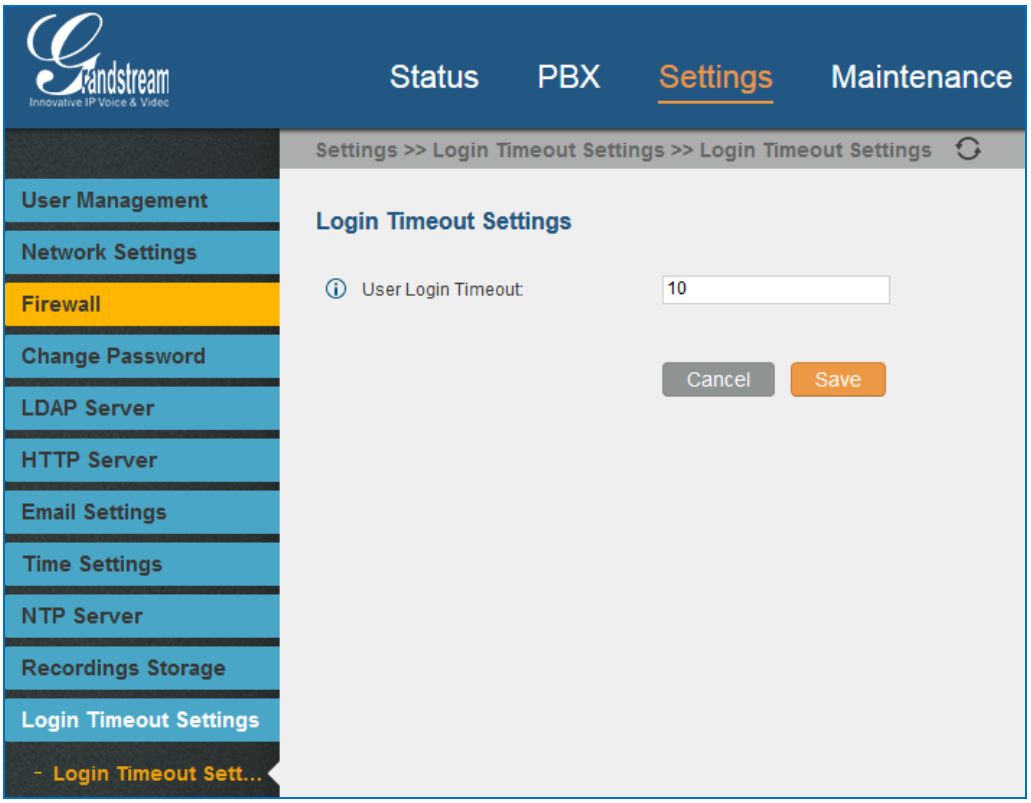


Figure 52: Login Timeout Settings

This page intentionally left blank

PROVISIONING

OVERVIEW

Grandstream SIP Devices can be configured via Web interface as well as via configuration file through TFTP/HTTP/HTTPS download. All Grandstream SIP devices support a proprietary binary format configuration file and XML format configuration file. The UCM6510 provides a Plug and Play mechanism to auto-provision the Grandstream SIP devices in a zero configuration manner by generating XML config file and having the phone to download it within LAN area. This allows users to finish the installation with ease and start using the SIP devices in a managed way.

To provision a phone, three steps are involved, i.e., discovery, configuration and provisioning. This section explains how Zero Config works on the UCM6510. The settings for this feature can be accessed via Web UI->**PBX**->**Zero Config**.

CONFIGURATION ARCHITECTURE FOR END POINT DEVICE

The end point device configuration in Zero Config is divided into the following three layers with priority from the lowest to the highest:

- **Global**

This is the lowest layer. Users can configure the most basic options that could apply to all Grandstream SIP devices during provisioning via Zero Config.

- **Model**

In this layer, users can define model-specific options for the configuration template.

- **Device**

This is the highest layer. Users can configure device-specific options for the configuration for individual device here.

Each layer also has its own structure in different levels. Please see figure below. The details for each layer are explained in sections ***[GLOBAL CONFIGURATION]***, ***[MODEL CONFIGURATION]*** and ***[DEVICE CONFIGURATION]***.

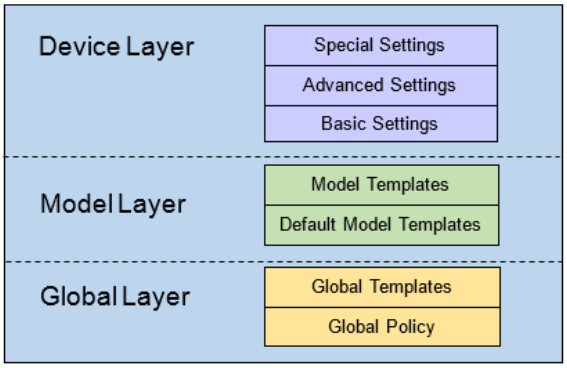


Figure 53: Zero Config Configuration Architecture for End Point Device

The configuration in model layer and device layer have all the options in global layers already, i.e., the options in global layer is a subset of the options in model layer and device layer. If an option is set in all three layers with different values, the highest layer value will override the value in lower layer. For example, if the user selects English for Language setting in Global Policy and Spanish for Language setting in Default Model Template, the language setting on the device to be provisioned will use Spanish as model layer has higher priority than global layer. To sum up, **configurations in higher layer will always override the configurations for the same options/fields in the lower layer when presented at the same time.**

After understanding the Zero Config configuration architecture, users could configure the available options for end point devices to be provisioned by the UCM6510 by going through the three layers. This configuration architecture allows users to set up and manage the Grandstream end point devices in the same LAN area in a centralized way.

AUTO PROVISIONING SETTINGS

By default, the Zero Config feature is enabled on the UCM6510 for auto provisioning. Two methods of auto provisioning are used.

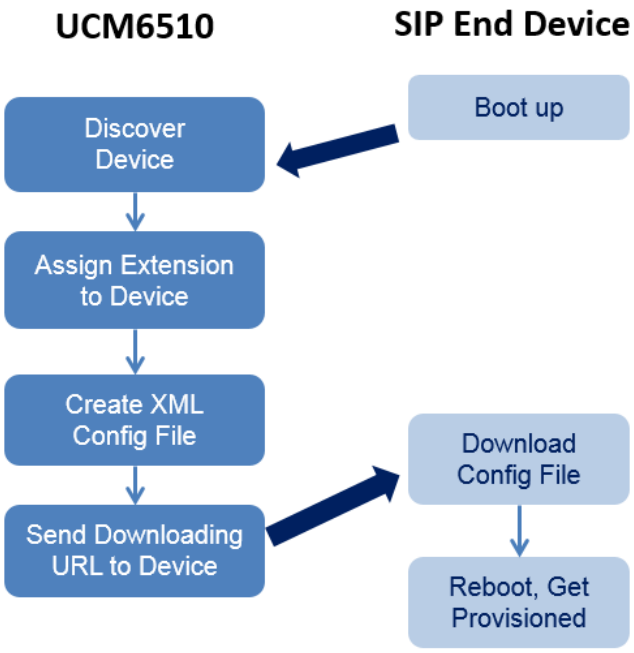


Figure 54: UCM6510 Zero Config

- **SIP SUBSCRIBE**

  When the phone boots up, it sends out SUBSCRIBE to a multicast IP address in the LAN. The UCM6510 discovers it and then sends a NOTIFY with the XML config file URL in the message body. The phone will then use the path to download the config file generated in the UCM6510 and take the new configuration.

- **DHCP OPTION 66**

  This method should be used only when the UCM6510 is set to "Route" mode under web GUI->**Settings**->**Network Settings**->**Basic Settings**: Method. When the phone restarts (by default DHCP Option 66 is turned on), it will send out a DHCP DISCOVER request. The UCM6510 receives it and returns DHCP OFFER with the config server path URL in the Option 66, for example, https://192.168.2.1:8089/zccgi/. The phone will then use the path to download the config file generated in the UCM6510.

To start the auto provisioning process, under Web GUI->**PBX**->**Zero Config**->**Zero Config Settings**, fill in the auto provision information.

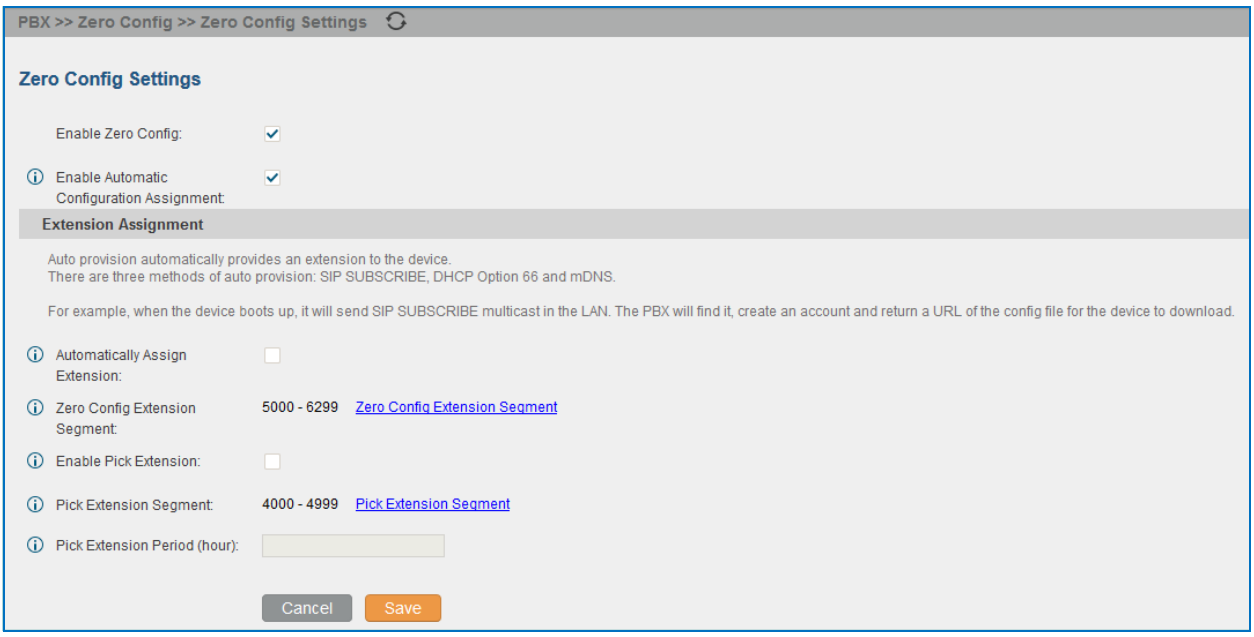

PBX >> Zero Config >> Zero Config Settings
Zero Config Settings
Enable Zero Config:
Enable Automatic Configuration Assignment:
Extension Assignment
Auto provision automatically provides an extension to the device.
There are three methods of auto provision: SIP SUBSCRIBE, DHCP Option 66 and mDNS.
For example, when the device boots up, it will send SIP SUBSCRIBE multicast in the LAN. The PBX will find it, create an account and return a URL of the config file for the device to download.
Automatically Assign Extension:
Zero Config Extension Segment:
5000 - 6299
Zero Config Extension Segment
Enable Pick Extension:
Pick Extension Segment:
4000 - 4999
Pick Extension Segment
Pick Extension Period (hour):
Cancel
Save

Figure 55: Auto Provision Settings

Table 22: Auto Provision Settings

Enable Zero Config	Enable or disable the Zero Config feature on the PBX. The default setting is enabled.
Enable Automatic Configuration Assignment	By default, this is disabled. If disabled, when SIP device boots up, the UCM6510 will only send the configuration path to the device when you have any manual configuration on the device. This manual configuration includes: - Any configuration under BASIC and CUSTOM page of the device in Zero Config page - If any global or model template (expect for the default template) is selected for the assigned device in Zero Config page. **Note:** When disabled, SIP devices can still be provisioned by manually sending NOTIFY from the UCM6510 which will include the XML config file URL for the SIP device to download.
Automatically Assign Extension	If enabled, when the device is discovered, the PBX will automatically assign an extension within the range defined in “Zero Config Extension Segment” to the device. The default setting is disabled.
Zero Config Extension Segment	Click on the link “Zero Config Extension Segment” to specify the extension range to be assigned if “Automatically Assign Extension” is enabled. The default range is 5000-6299. Zero Config Extension Segment range can be

	defined in web UI->**PBX**->**Internal Options**->**General** page->Extension Preference section: “Auto Provision Extensions”.
Enable Pick Extension	If enabled, the extension list will be sent out to the device after receiving the device’s request. This feature is for the GXP series phones that support selecting extension to be provisioned via phone’s LCD. The default setting is disabled.
Pick Extension Segment	Click on the link “Pick Extension Segment” to specify the extension list to be sent to the device. The default range is 4000 to 4999. Pick Extension Segment range can be defined in web UI->**PBX**->**Internal Options**->**General** page->Extension Preference section: “Pick Extensions”.
Pick Extension Period (hour):	Specify the number of minutes to allow the phones being provisioned to pick extensions.

Please make sure an extension is manually assigned to the phone or “Automatically Assign Extension” is enabled during provisioning. After the configuration on the UCM6510 web GUI, click on “Save” and “Apply Changes”. Once the phone boots up and picks up the config file from the UCM6510, it will take the configuration right away.

DISCOVERY

Users could manually discover the device by specifying the IP address or scanning the entire LAN network. Three methods are supported to scan the devices.

- PING
- ARP
- SIP Message (NOTIFY)

Click on “Auto Discover” under web **GUI-> PBX-> Zero Config-> Zero Config**, fill in the “Scan Method” and “Scan IP”. The IP address segment will be automatically filled in based on the network mask detected on the UCM6510. If users need scan the entire network segment, enter 255 (for example, 192.168.40.255) instead of a specific IP address. Then click on “Save” to start discovering the devices within the same network. To successfully discover the devices, “Zero Config” needs to be enabled on the UCM6510 web GUI->**PBX**->**Zero Config**->**Auto Provisioning Settings**.

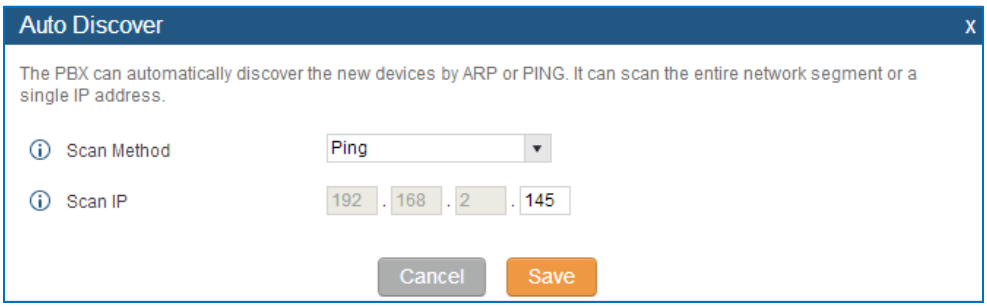
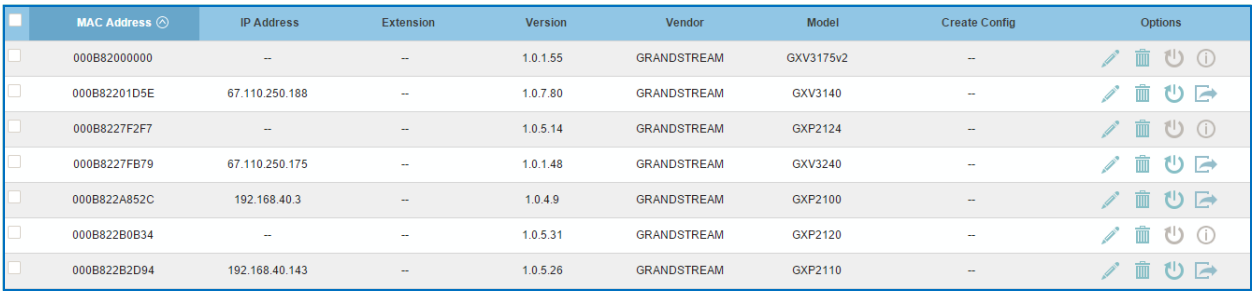

Auto Discover
x
The PBX can automatically discover the new devices by ARP or PING. It can scan the entire network segment or a single IP address.
Scan Method
Ping
Scan IP
192 . 168 . 2 . 145
Cancel
Save

Figure 56: Auto Discover

The following figure shows a list of discovered phones. The MAC address, IP Address, Extension (if assigned), Version, Vendor, Model, Connection Status, Create Config, Options (Edit/Delete/Update) are displayed in the list.



MAC Address	IP Address	Extension	Version	Vendor	Model	Create Config	Options
000B82000000	--	--	1.0.1.55	GRANDSTREAM	GXV3175v2	--	
000B82201D5E	67.110.250.188	--	1.0.7.80	GRANDSTREAM	GXV3140	--	
000B8227F2F7	--	--	1.0.5.14	GRANDSTREAM	GXP2124	--	
000B8227FB79	67.110.250.175	--	1.0.1.48	GRANDSTREAM	GXV3240	--	
000B822A852C	192.168.40.3	--	1.0.4.9	GRANDSTREAM	GXP2100	--	
000B822B0B34	--	--	1.0.5.31	GRANDSTREAM	GXP2120	--	
000B822B2D94	192.168.40.143	--	1.0.5.26	GRANDSTREAM	GXP2110	--	

Figure 57: Discovered Devices

GLOBAL CONFIGURATION

GLOBAL POLICY

Global configuration will apply to all the connected Grandstream SIP end point devices in the same LAN with the UCM6510 no matter what the Grandstream device model it is. It is divided into two levels:

- Web UI->**PBX->Zero Config->Global Policy**
- Web UI->**PBX->Zero Config->Global Templates**.
- **Global Templates** configuration has higher priority to **Global Policy** configuration.

Global Policy can be accessed in web GUI->**PBX->Zero Config->Global Policy** page. On the top of the configuration table, users can select category in the “Options” dropdown list to quickly navigate to the category. The categories are:

- **Localization**: configure display language, data and time.
- **Phone Settings**: configure dial plan, call features, NAT, call progress tones and etc.

- **Contact List**: configure LDAP and XML phonebook download.
- **Maintenance**: configure upgrading, web access, Telnet/SSH access and syslog.
- **Network Settings**: configure IP address, QoS and STUN settings.
- **Customization**: customize LCD screen wallpaper for the supported models.

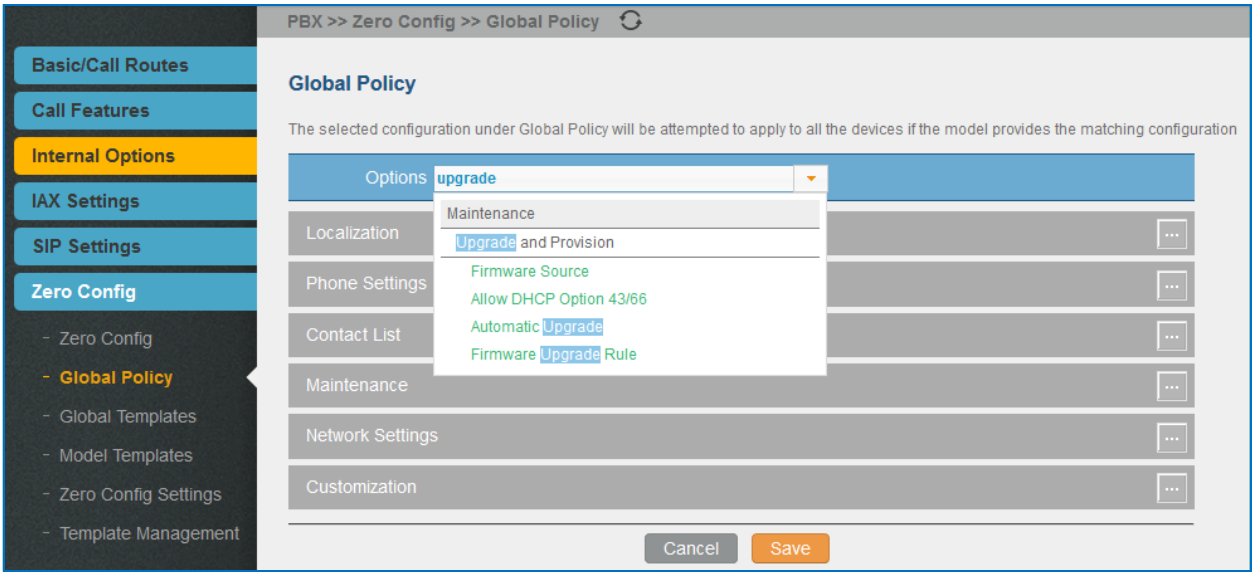


Figure 58: Global Policy Categories

Select the checkbox on the left of the parameter you would like to configure to active the dropdown list for this parameter.

The following tables list the Global Policy configuration parameters for the SIP end device.

Table 23: Global Policy Parameters – Localization

Language settings	
Language	Select the LCD display language on the SIP end device.
Date and Time	
Date Format	Configure the date display format on the SIP end device's LCD.
Time Format	Configure the time display in 12-hour or 24-hour format on the SIP end device's LCD.
NTP Server	Configure the URL or IP address of the NTP server. The SIP end device may obtain the date and time from the server.
Time Zone	Configure the time zone used on the SIP end device.

Table 24: Global Policy Parameters – Phone Settings

Default Call Settings	
Dial Plan	Configure the default dial plan rule. For syntax and examples, please refer to user manual of the SIP devices to be provisioned for more details.
Enable Call Features	When enabled, “Do Not Disturb”, “Call Forward” and other call features can be used via the local feature code on the phone. Otherwise, the ITSP feature code will be used.
Use # as Dial Key	If set to “Yes”, pressing the number key “#” will immediately dial out the input digits.
Auto Answer by Call-info	If set to “Yes”, the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info header sent from the server/proxy. The default setting is enabled.
NAT Traversal	Configure if NAT traversal mechanism is activated.
User Random Port	If set to “Yes”, this parameter will force random generation of both the local SIP and RTP ports.
General Settings	
Call Progress Tones	Configure call progress tones including ring tone, dial tone, second dial tone, message waiting tone, ring back tone, call waiting tone, busy tone and reorder tone using the following syntax: f1=val, f2=val[, c=on1/ off1[- on2/ off2[- on3/ off3]]]; • Frequencies are in Hz and cadence on and off are in 10ms). • “on” is the period (in ms) of ringing while “off” is the period of silence. Up to three cadences are supported. • Please refer to user manual of the SIP devices to be provisioned for more details
HEADSET Key Mode	Select “Default Mode” or “Toggle Headset/Speaker” for the Headset key. Please refer to user manual of the SIP devices to be provisioned for more details.

Table 25: Global Policy Parameters – Contact List

LDAP Phonebook	
Source	Select “Manual” or “PBX” as the LDAP configuration source. • If “Manual” is selected, the LDAP configuration below will be applied to the SIP end device. • If “PBX” is selected, the LDAP configuration built-in from UCM6510 web UI->**Settings**->**LDAP Server** will be applied.

Address	Configure the IP address or DNS name of the LDAP server.
Port	Configure the LDAP server port. The default value is 389.
Base DN	This is the location in the directory where the search is requested to begin. Example: • dc=grandstream, dc=com • ou=Boston, dc=grandstream, dc=com
User Name	Configure the bind “Username” for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
Password	Configure the bind “Password” for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
Number Filter	Configure the filter used for number lookups. Please refer to user manual for more details.
Name Filter	Configure the filter used for name lookups. Please refer to user manual for more details.
Version	Select the protocol version for the phone to send the bind requests. The default value is 3.
Name Attribute	Specify the “name” attributes of each record which are returned in the LDAP search result. Example: • gn • cn sn description
Number Attribute	Specify the “number” attributes of each record which are returned in the LDAP search result. Example: • telephoneNumber • telephoneNumber Mobile
Display Name	Configure the entry information to be shown on phone’s LCD. Up to 3 fields can be displayed. Example: • %cn %sn %telephoneNumber
Max Hits	Specify the maximum number of results to be returned by the LDAP server. Valid range is 1 to 3000. The default value is 50.
Search Timeout	Specify the interval (in seconds) for the server to process the request and client waits for server to return. Valid range is 0 to 180. The default value is 30.
Sort Results	Specify whether the searching result is sorted or not. The default setting is No.
Incoming Calls	Configure to enable LDAP number searching when receiving calls. The default setting is No.
Outgoing Calls	Configure to enable LDAP number searching when making calls. The default setting is No.

Lookup Display Name	Configures the display name when LDAP looks up the name for incoming call or outgoing call. It must be a subset of the LDAP Name Attributes.
XML Phonebook	
Phonebook XML Server	Select the source of the phonebook XML server. • Disable Disable phonebook XML downloading. • Manual Once selected, users need specify downloading protocol HTTP, HTTPS or TFTP and the server path to download the phonebook XML file. The server path could be IP address or URL, with up to 256 characters. • Local UCM Server Once selected, click on the Server Path field to upload the phonebook XML file. Please note: after uploading the phonebook XML file to the server, the original file name will be used as the directory name and the file will be renamed as phonebook.xml under that directory.
Phonebook Download Interval	Configure the phonebook download interval (in Minute). If set to 0, automatic download will be disabled. Valid range is 5 to 720.
Remove manually-edited entries on download	If set to “Yes”, when XML phonebook is downloaded, the entries added manually will be automatically removed.

Table 26: Global Policy Parameters – Maintenance

Upgrade and Provision	
Firmware Source	Firmware source via ZeroConfig provisionoing could a URL for external server address, local UCM directory or USB media if plugged in to the UCM6510. Select a source to get the firmware file: • URL If select to use URL to upgrade, complete the configuration for the following four parameters: “Upgrade Via”, “Server Path”, “File Prefix” and “File Postfix”. • Local UCM Server Firmware can be uploaded to the UCM6510 internal storage for firmware upgrade. If selected, click on “Manage Storage” icon next to “Directory” option, upload firmware file and select directory for the end device to retrieve the firmware file. • Local USB Media If selected, the USB storage device needs to be plugged into the UCM6510 and the firmware file must be put under a folder named

	"ZC_firmware" in the USB storage root directory. • Local SD Card Media If selected, an SD card needs to be plugged into the UCM6510 and the firmware file must be put under a folder named "ZC_firmware" in the USB storage root directory.
Upgrade via	When URL is selected as firmware source, configure upgrade via TFTP, HTTP or HTTPS.
Server Path	When URL is selected as firmware source, configure the firmware upgrading server path.
File Prefix	When URL is selected as firmware source, configure the firmware file prefix. If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the phone, if URL is selected as firmware source.
File Postfix	When URL is selected as firmware source, configure the firmware file postfix. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
Allow DHCP Option 43/66	If DHCP option 43 or 66 is enabled on the LAN side, the TFTP server can be redirected.
Automatic Upgrade	If enabled, the end point device will automatically upgrade if a new firmware is detected. Users can select automatic upgrading by day, by week or by minute. • By week Once selected, specify the day of the week to check HTTP/TFTP server for firmware upgrades or configuration files changes. • By day Once selected, specify the hour of the day to check the HTTP/TFTP server for firmware upgrades or configuration files changes. • By minute Once selected, specify the interval **X** that the SIP end device will request for new firmware every **X** minutes.
Firmware Upgrade Rule	Specify how firmware upgrading and provisioning request to be sent.
Web Access	
Admin Password	Configure the administrator password for admin level login.
End-User Password	Configure the end-user password for the end user level login.
Web Access Mode	Select HTTP or HTTPS as the web access protocol.
Web Server Port	Configure the port for web access. The valid range is 1 to 65535.
Security	
Disable Telnet/SSH	Enable Telnet/SSH access for the SIP end device. If the SIP end device

	supports Telnet access, this option controls the Telnet access of the device; if the SIP end device supports SSH access, this option controls the SSH access of the device.
Syslog	
Syslog Server	Configure the URL/IP address for the syslog server.
Syslog Level	Select the level of logging for syslog.
Send SIP Log	Configure whether the SIP log will be included in the syslog message.

Table 27: Global Policy Parameters – Network Settings

Basic Settings	
IP Address	Configure how the SIP end device shall obtain the IP address. DHCP or PPPoE can be selected. • DHCP Once selected, users can specify the Host Name (option 12) of the SIP end device as DHCP client, and Vendor Class ID (option 60) used by the client and server to exchange vendor class ID information. • PPPoE Once selected, users need specify the Account ID, Password and Service Name for PPPoE.
Advanced Setting	
Layer 3 QoS	Define the Layer 3 QoS parameter. This value is used for IP Precedence, Diff-Serv or MPLS. Valid range is 0-63.
Layer 2 QoS Tag	Assign the VLAN Tag of the Layer 2 QoS packets. Valid range is 0 -4095.
Layer 2 QoS Priority Value	Assign the priority value of the Layer 2 QoS packets. Valid range is 0-7.
STUN Server	Configure the IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
Keep Alive Interval	Specify how often the phone will send a blank UDP packet to the SIP server in order to keep the “ping hole” on the NAT router to open. Valid range is 10-160.

Table 28: Global Policy Parameters – Customization

Wallpaper	
Screen Resolution 1024 x 600	Check this option if the SIP end device shall use 1024 x 600 resolution for the LCD screen wallpaper. • Source Configure the location where wallpapers are stored. • File If “URL” is selected as source, specify the URL of the wallpaper file. If

	"Local UCM Server" is selected as source, click to upload wallpaper file to the UCM6510.
Screen Resolution 800 x 400	Check this option if the SIP end device shall use 800 x 400 resolution for the LCD screen wallpaper. • Source Configure the location where wallpapers are stored. • File If "URL" is selected as source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as source, click to upload wallpaper file to the UCM6510.
Screen Resolution 480 x 272	Check this option if the SIP end device shall use 480 x 272 resolution for the LCD screen wallpaper. • Source Configure the location where wallpapers are stored. • File If "URL" is selected as source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as source, click to upload wallpaper file to the UCM6510.
Screen Resolution 320 x 240	Check this option if the SIP end device supports 320 x 240 resolution for the LCD screen wallpaper. • Source Configure the location where wallpapers are stored. • File If "URL" is selected as source, specify the URL of the wallpaper file. If "Local UCM Server" is selected as source, click to upload wallpaper file to the UCM6510.

GLOBAL TEMPLATES

Global Templates can be accessed in web GUI->**PBX**->**Zero Config**->**Global Templates**. Users can create multiple global templates with different sets of configurations and save the templates. Later on, when the user configures the device in Edit Device dialog->Advanced Settings, the user can select to use one of the global template for the device. Please refer to section *[*MANAGE DEVICES*]* for more details on using the global templates.

When creating global template, users can select the categories and the parameters under each categories to be used in the template. The global policy and the selected global template will both take effect when generating the config file. However, the selected global template has higher priority to the global policy

when it comes to the same setting option/field. If the same option/field has different value configured in the global policy and the selected global template, the value for this option/field in the selected global template will override the value in global policy.

- Click on “Create New Template” to add a global template. Users will see the following configurations.

Table 29: Create New Template

Template Name	Create a name to identify this global template.
Description	Provide a description for the global template. This is optional.
Active	Check this option to enable the global template.

- Click on to edit the global template.

  The window for editing global template is shown in the following figure. In the “Options” field, after entering the option name key word, the options containing the key word will be listed. Users could then select the options to be modified and click on “Add Option” to add it into the global template.

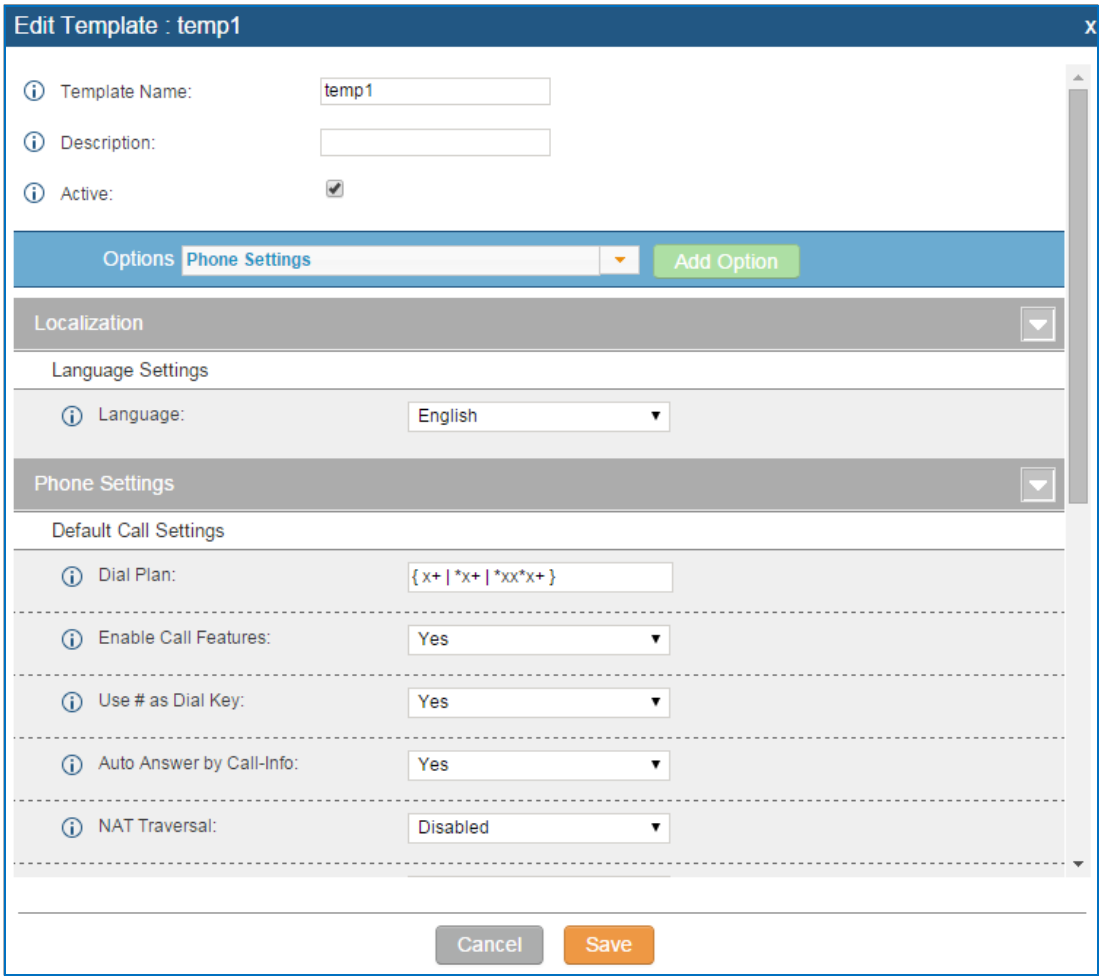


Figure 59: Edit Global Template

The added options will show in the list. Users can then enter or select value for each option to be used in the global template. On the left side of each added option, users can click on to remove this option from the template. On the right side of each option, users can click on to reset the option value to the default value.

- Click on "Save" to save this global template.
- The created global templates will show in the web UI->**PBX**->**Zero Config**->**Global Templates** page. Users can click on to delete the global template or click on "Delete Selected Templates" to delete multiple selected templates at once.
- Click on "Toggle Selected Template(s)" to toggle the status between enabled/disabled for the selected templates.

MODEL CONFIGURATION

MODEL TEMPLATES

Model layer configuration allows users to apply model-specific configurations to different devices. Users could create/edit/delete a model template by accessing web GUI, page **PBX->Zero Config->Model Templates**. If multiple model templates are created and enabled, when the user configures the device in Edit Device dialog->Advanced Settings, the user can select to use one of the model template for the device. Please refer to section *[*MANAGE DEVICES*]* for more details on using the model template.

For each created model template, users can assign it as default model template. If assigned as default model template, the values in this model template will be applied to all the devices of this model. There is always only one default model template that can be assigned at one time on the UCM6510.

The selected model template and the default model template will both take effect when generating the config file for the device. However the model template has higher priority to default model template when it comes to the same setting option/field. If the same option/field has different value configured in the default model template and the selected model template, the value for this option/field in the selected model template will override the value in default model template.

- Click on "Create New Template" to add a model template.

Table 30: Create New Model Template

Model	Select a model to apply this template. The supported Grandstream models are listed in the dropdown list for selection.
Template Name	Create a name for the model template.
Description	Enter a description for the model template. This is optional.
Default Model Template	Select to assign this model template as the default model template. The value of the option in default model template will be overridden if other selected model template has a different value for the same option.
Active	Check this option to enable the model template.

- Click on to edit the model template.

  The editing window for model template is shown in the following figure. In the “Options” field, enter the option name key word, the option that contains the key word will be listed. User could then select the option and click on “Add Option” to add it into the model template.

  Once added, the option will be shown in the list below. On the left side of each option, users can click on to remove this option from the model template. On the right side of each option, users can click on to reset the option to the default value.

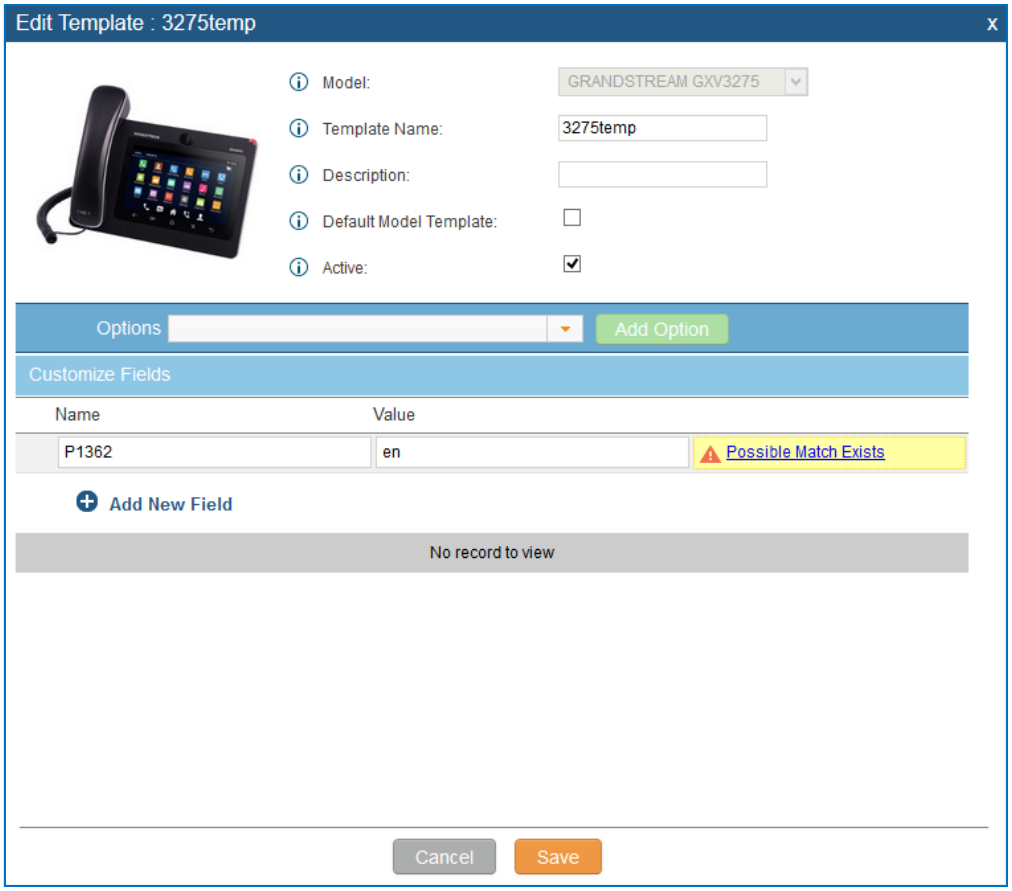


Figure 60: Edit Model Template

User could also click on "Add New Field" to add a P value number and the value to the configuration. The following figure shows setting P value "P1362" to "en", which means the display language on the LCD is set to English. For P value information of different models, please refer to configuration template here http://www.grandstream.com/support/tools.

- Click on Save when done. The model template will be displayed on web UI->**PBX->Zero Config->Model Templates** page.
- Click on to delete the model template or click on "Delete Selected Templates" to delete multiple selected templates at once.
- Click on "Toggle Selected Template(s)" to toggle the status between enabled/disabled for the selected model templates.

MODEL UPDATE

UCM6510 zero config feature supports provisioning all models of Grandstream SIP end devices. Templates for most of the Grandstream models are built in with the UCM6510 already. Templates for GXP16XX, GSWave and Surveillance products requires user to download on UCM6510 web UI->**PBX**->**Zero Config**->**Model Update** first as those products are more often used as needed. After downloading the model template, it will show in the dropdown list for "Model" selection when editing the model template.

- Click on to download the template.
- User could also upload model template package to UCM6510.

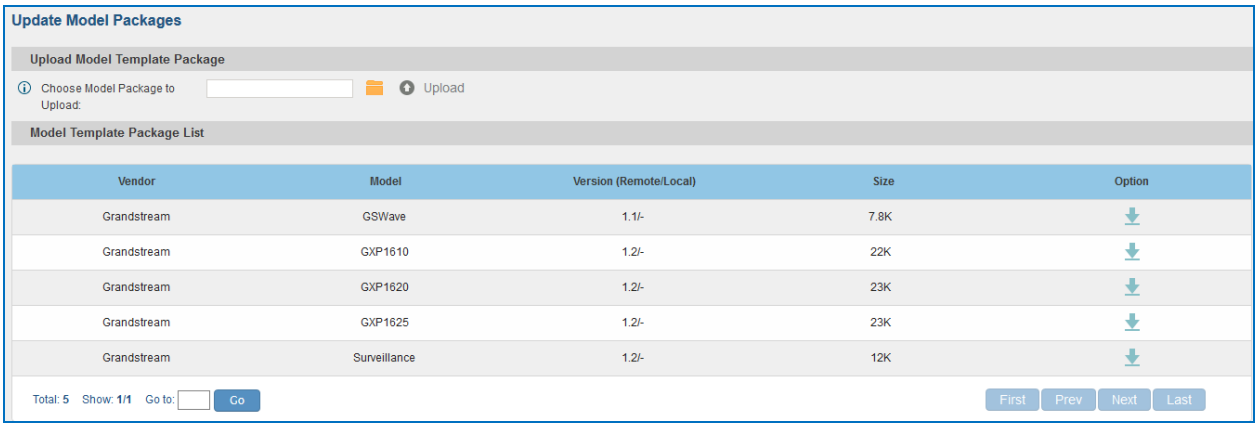


Figure 61: Template Management

DEVICE CONFIGURATION

On web GUI, page **PBX->Zero Config->Zero Config**, users could create new device, delete existing device(s), make special configuration for a single device, or send NOTIFY to existing device(s).

CREATE NEW DEVICE

Besides configuring the device after the device is discovered, users could also directly create a new device and configure basic settings before the device is discovered by the UCM6510. Once the device is plugged in, it can then be discovered and provisioned. This gives the system administrator adequate time to set up each device beforehand.

Click on "Create New Device" and the following dialog will show. Follow the steps below to create the configurations for the new device.

1. Firstly select a model for the device to be created and enter its MAC address, IP address and firmware version (optional) in the corresponding field.
2. Basic settings will show a list of settings based on the model selected in step 1. Users could assign extensions to accounts, assign functions to Line Keys and Multiple-Purposed Keys if supported on the selected model.
3. Click on “Create New Device” to save the configuration for this device.

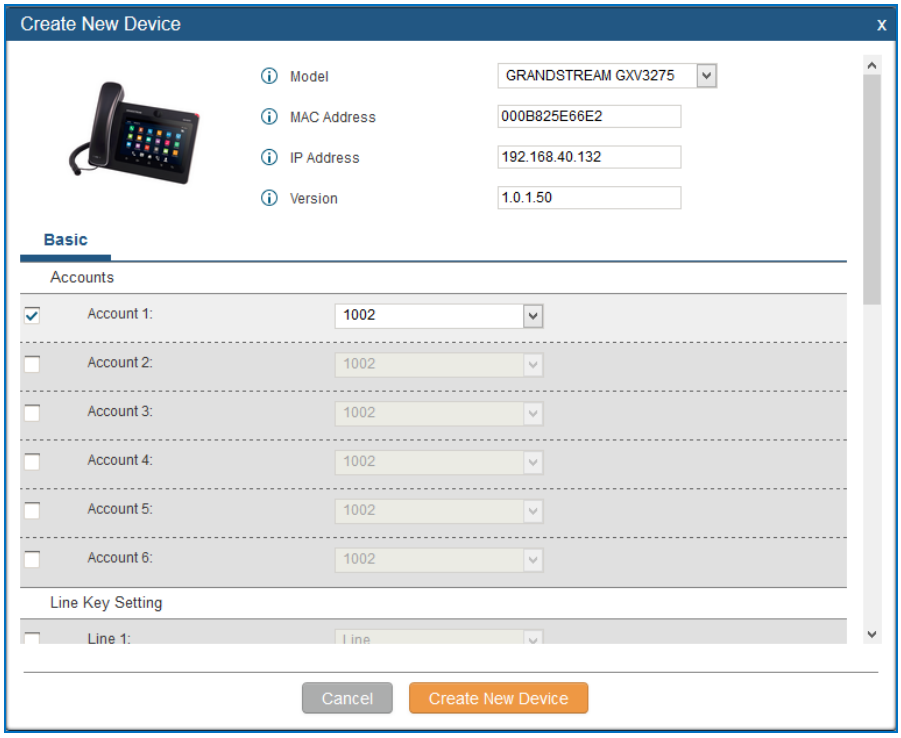


Figure 62: Create New Device

MANAGE DEVICES

The device manually created or discovered from Auto Discover will be listed in the web UI->**PBX**->**Zero Config**->**Zero Config** page. Users can see the devices with their MAC address, IP address, vendor, model and etc.

Figure 63: Manage Devices

1. Click on to access the web UI of the phone.

2. Click on to edit the device configuration.

A new dialog will be displayed for the users to configure “Basic” settings and “Advanced” settings. “Basic” settings have the same configurations as displayed when manually creating a new device, i.e., account, line key and MPK settings; “Advanced” settings allow users to configure more details in a five-level structure.

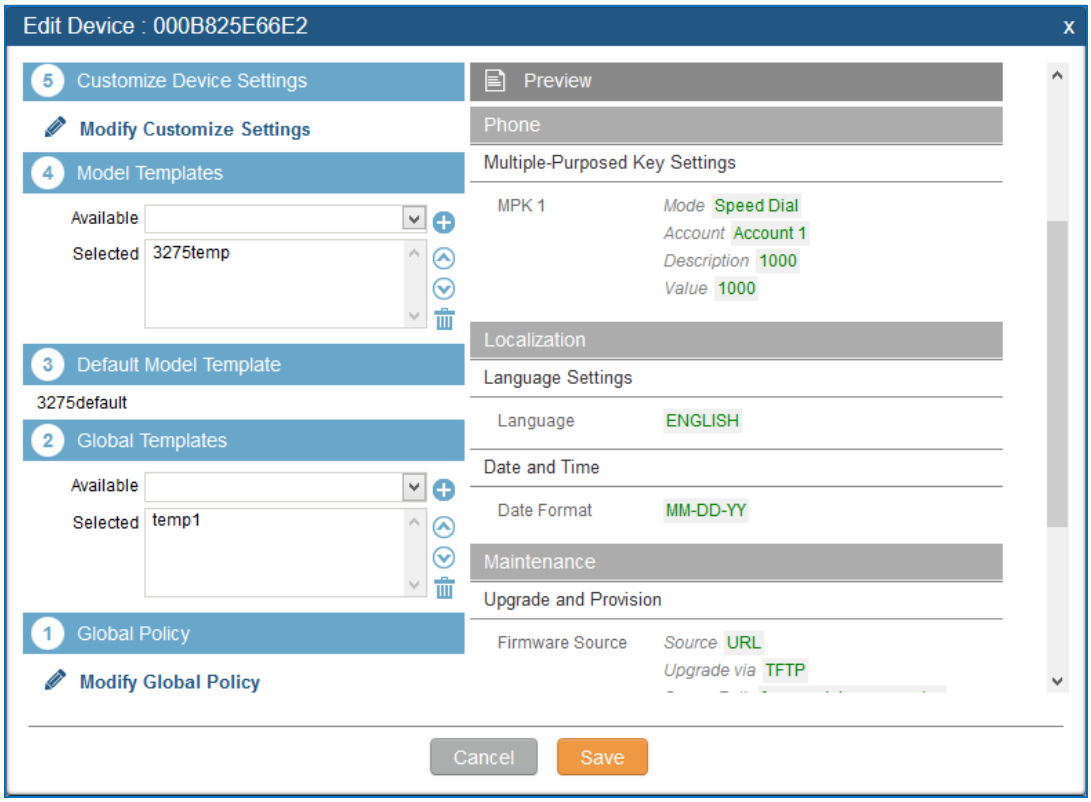


Figure 64: Edit Device

A preview of the “Advanced” settings is shown in the above figure. There are five levels configurations as described in (1) (2) (3) (4) (5) below, with priority from the lowest to the highest. The configurations in all levels will take effect for the device. If there are same options existing in different level configurations with different value configured, the higher level configuration will override the lower level configuration.

(1) Global Policy

This is the lowest level configuration. The global policy configured in web UI->**PBX->Zero Config->Global Policy** will be applied here. Clicking on “Modify Global Policy” to redirect to page **PBX->Zero Config->Global Policy**.

(2) Global Templates

Select a global template to be used for the device and click on to add. Multiple global templates can be selected and users can arrange the priority by adjusting orders via and .

All the selected global templates will take effect. If the same option exists on multiple selected global templates, the value in the template with higher priority will override the one in the template with lower priority. Click on to remove the global template from the selected list.

(3) Default Model Template

Default Model Template will be applied to the devices of this model. Default model template can be configured in model template under web UI->**PBX**->**Zero Config**->**Model Templates** page. Please see default model template option in ***[Table 30: Create New Model Template]***.

(4) Model Templates

Select a model template to be used for the device and click on to add. Multiple global templates can be selected and users can arrange the priority by adjusting orders via and . All the selected model templates will take effect. If the same option exists on multiple selected model templates, the value in the template with higher priority will override the one in the template with lower priority. Click on to remove the model template from the selected list.

(5) Customize Device Settings

This is the highest level configuration in the “Advanced” settings of the device. Click on “Modify Customize Device Settings” and following dialog will show.

Figure 65: Edit Customize Device Settings

Scroll down in the dialog to view and edit the device-specific options. If the users would like to add more options which are not in the pre-defined list, click on “Add New Field” to add a P value number and the value to the configuration. The following figure shows setting P value “P1362” to “en”, which means the display language on the LCD is set to English.

The warning information next to the P value field indicates that the option matching the P value number exists in the configuration already.

For P value information of different models, please refer to configuration template here http://www.grandstream.com/support/tools.

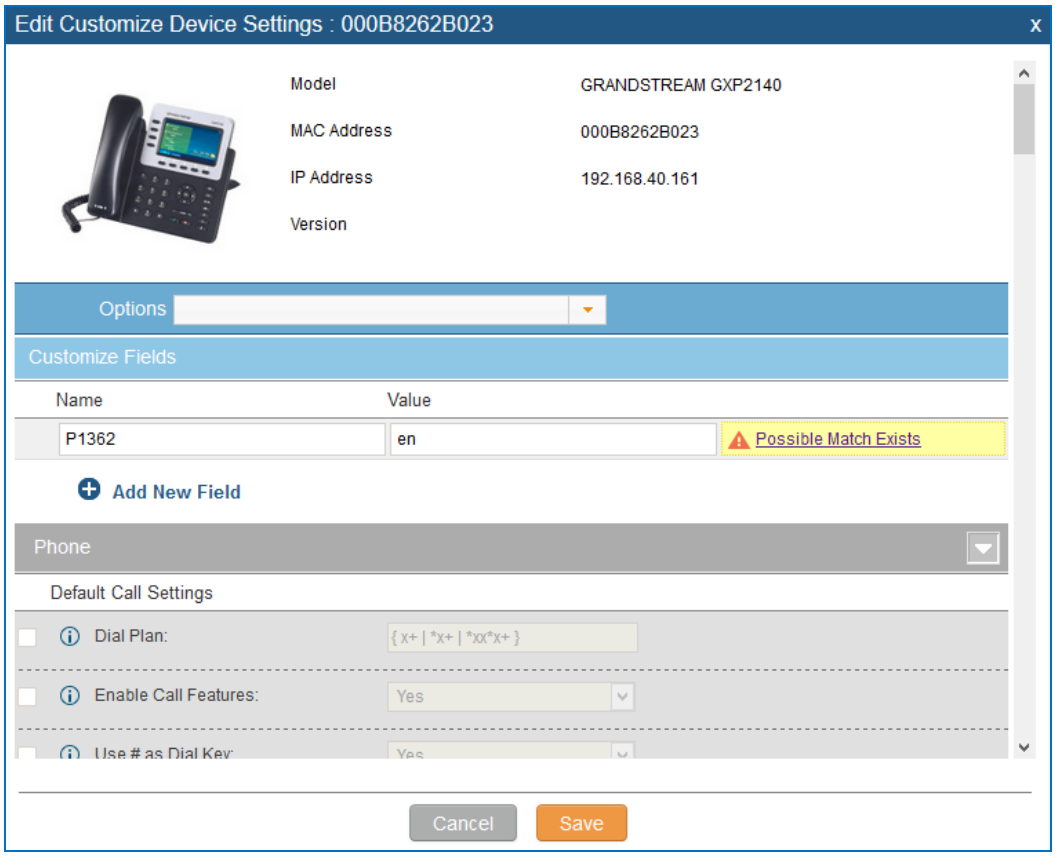


Figure 66: Add P Value in Customize Device Settings

- Select multiple devices that need to be modified and then click on Modify Selected Devices to batch modify devices.

  If selected devices are of the same model, the configuration dialog is like the following figure. Configurations in five levels are all available for users to modify.

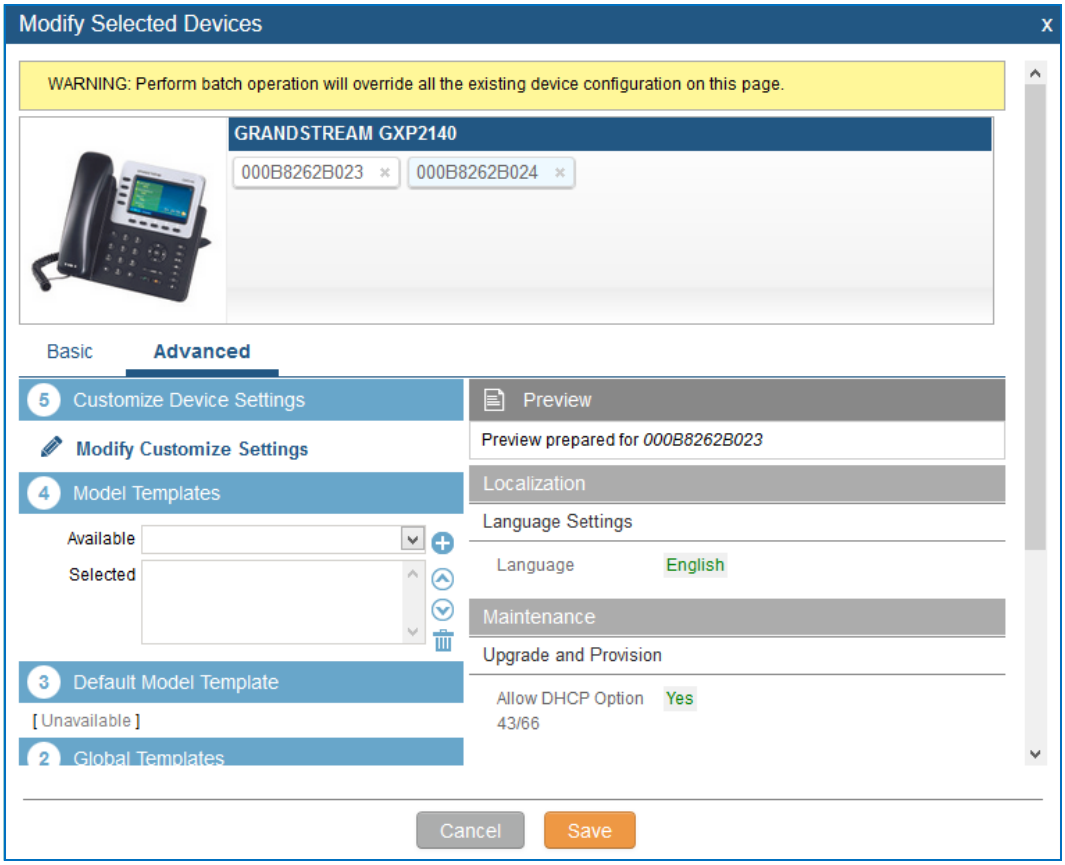


Figure 67: Modify Selected Devices–Same Model

If selected devices are of different models, the configuration dialog is like the following figure. Click on to view more devices of other models. Users are only allowed to make modifications in Global Templates and Global Policy level.

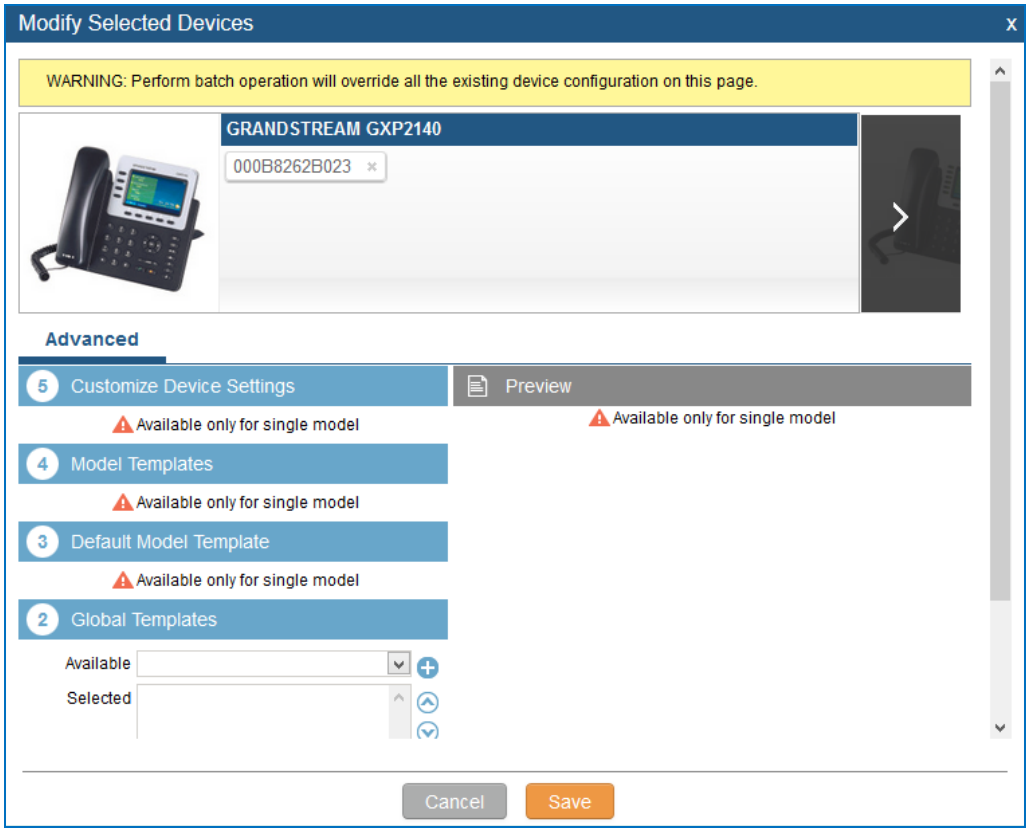


Figure 68: Modify Selected Devices—Different Models

Warning:

Perform batch operation will override all the configurations made when editing a single device. For example, if the user configures a GXP2140 to use template "TempA" in Global Templates level by editing a single device and then selects several devices including that GXP2140 to batch modify devices selecting "TempB" in Global Templates level, the user will see the global templates changed to "TempB" when viewing the configurations for the GXP2140.

After the above configurations, save the changes and go back to web UI->**PBX**->**Zero Config**->**Zero Config** page. Users could then click on to send NOTIFY to the SIP end point device and trigger the provisioning process. The device will start downloading the generated configuration file from the URL contained in the NOTIFY message.

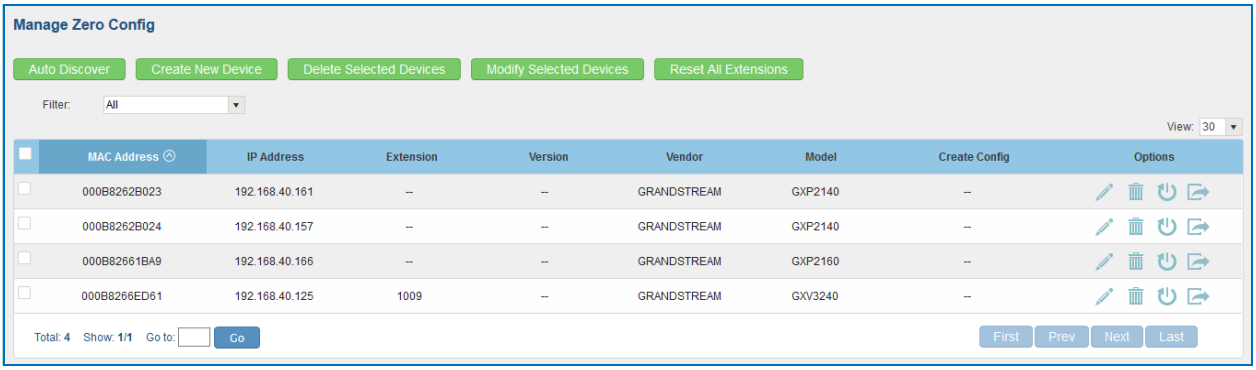


Figure 69: Device List in Zero Config

In this web page, users can also click on “Reset All Extensions” to reset the extensions of all the devices.

SAMPLE APPLICATION

Assuming in a small business office where there are 8 GXP2140 phones used by customer support and 1 GXV3275 phone used by customer support supervisor. 3 of the 8 customer support members speak Spanish and the rest speak English. We could deploy the following configurations to provisioning the office phones for the customer support team.

1. Go to web GUI->**PBX**->**Zero Config**->**Auto Provision Settings**, select “Enable Zero Config”.

2. Go to web GUI->**PBX**->**Zero Config**->**Global Policy**, configure Date Format, Time Format and Firmware Source as follows.

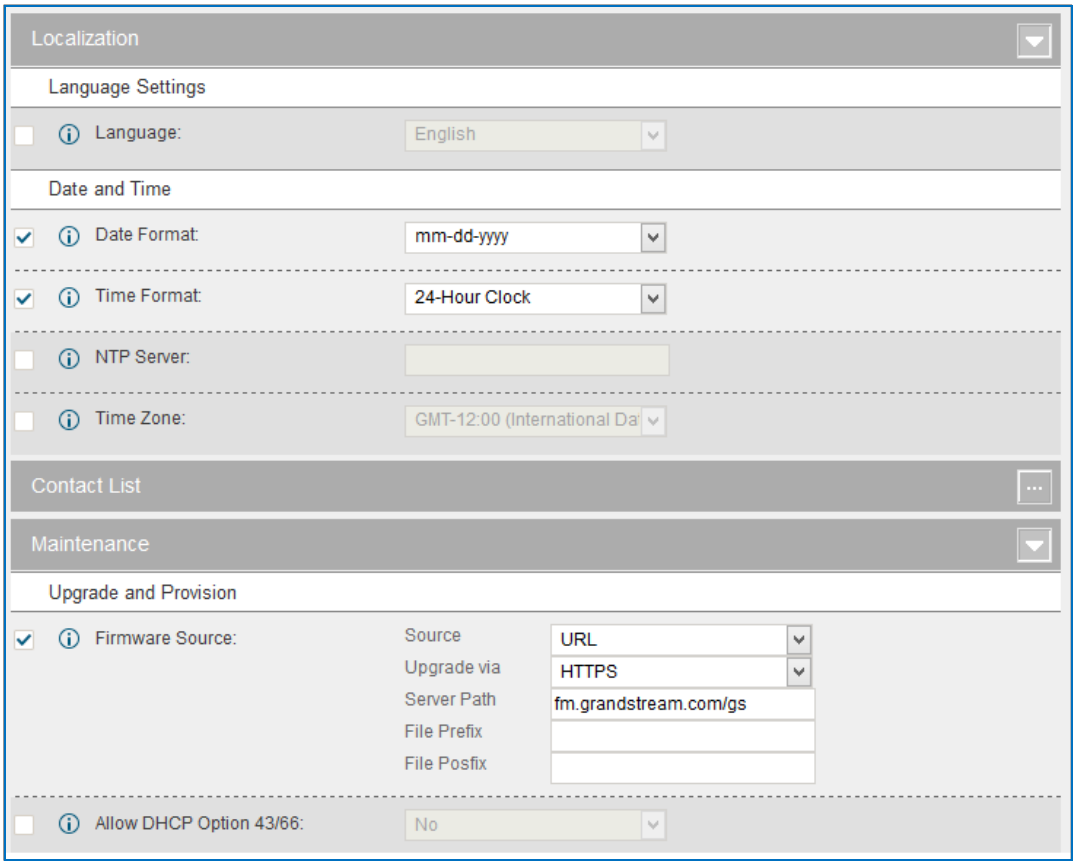


Figure 70: Zero Config Sample – Global Policy

3. Go to web GUI->**PBX**->**Zero Config**->**Model Templates**, create a new model template "English Support Template" for GXP2140. Add option "Language" and set it to "English". Then select the option "Default Model Template" to make it the default model template.

4. Go to web GUI->**PBX**->**Zero Config**->**Model Templates**, create another model template "Spanish Support Template" for GXP2140. Add option "Language" and set it to "Español".

5. After 9 devices are powered up and connected to the LAN network, use "Auto Discover" function or "Create New Device" function to add the devices to the device list on web UI->**PBX**->**Zero Config**->**Zero Config**.

6. On web GUI->**PBX**->**Zero Config**->**Zero Config** page, users could identify the devices by their MAC addresses or IP addresses displayed on the list. Click on to edit the device settings.

7. For each of the 5 phones used by English speaking customer support, in “Basic” settings select an available extension for account 1 and click on “Save”. Then click on “Advanced” settings tab to bring up the following dialog. Users will see the English support template is applied since this is the default model template. A preview of the device settings will be listed on the right side.

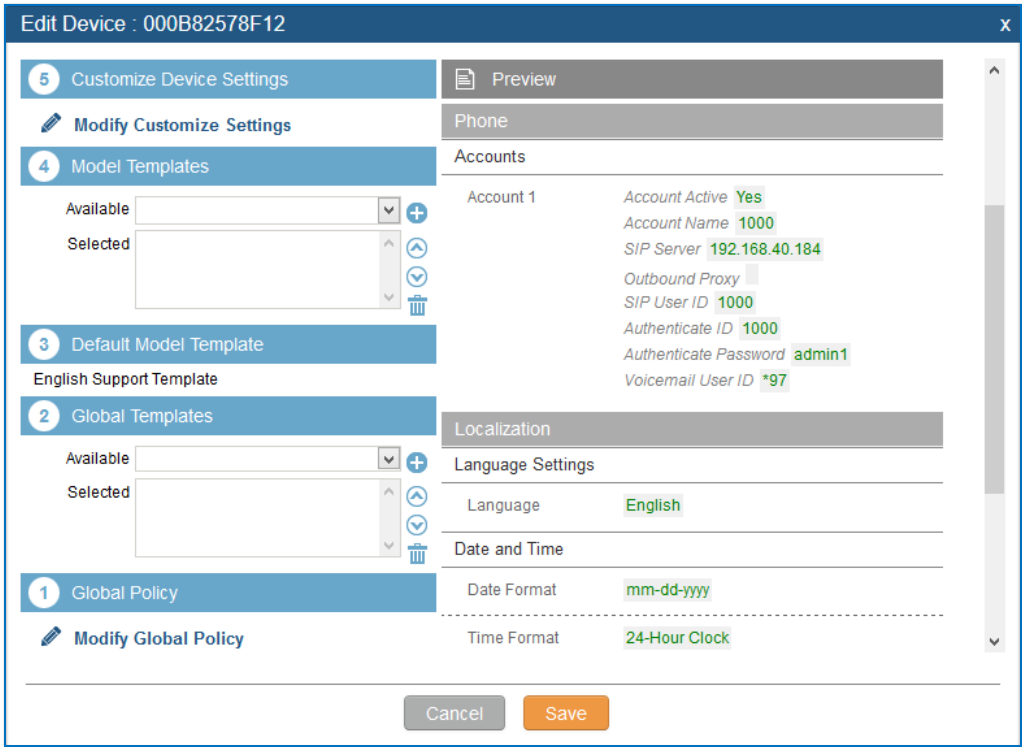


Figure 71: Zero Config Sample – Device Preview 1

8. For the 3 phones used by Spanish support, in “Basic” settings select an available extension for account 1 and click on “Save”. Then click on “Advanced” settings tab to bring up the following dialog.

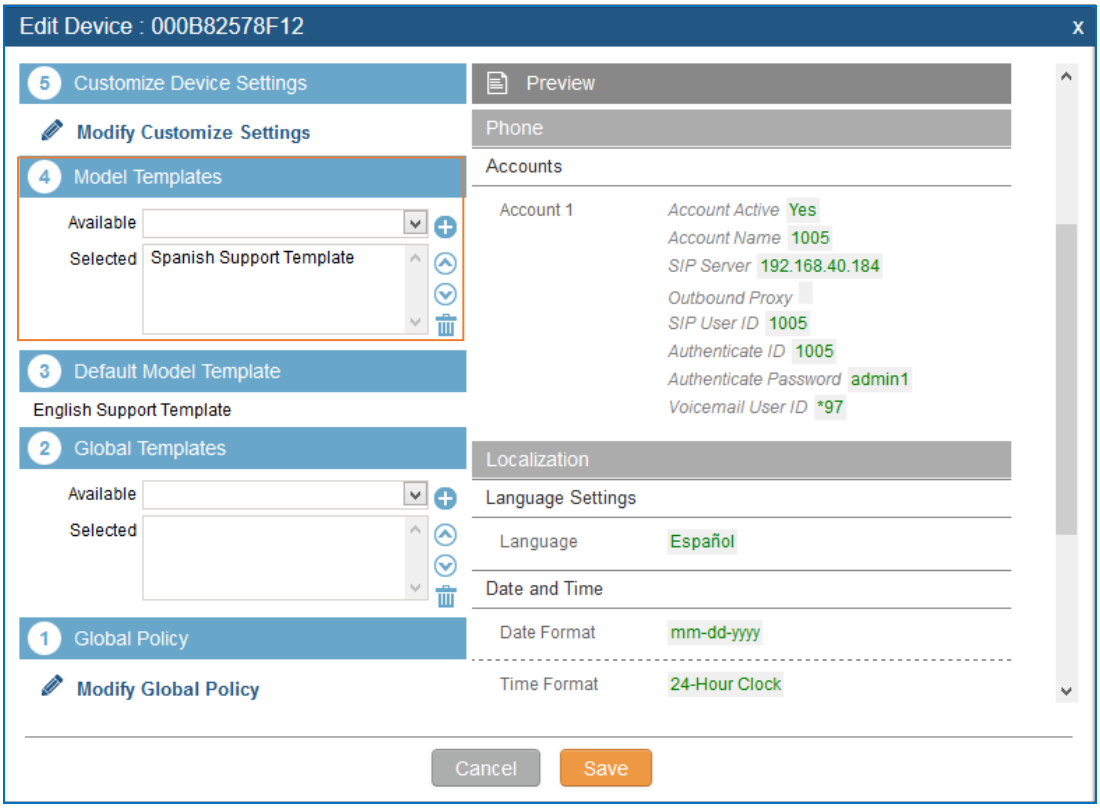


Figure 72: Zero Config Sample – Device Preview 2

Select "Spanish Support Template" in "Model Template". The preview of the device settings is displayed on the right side and we can see the language is set to "Español" since Model Template has the higher priority for the option "Language", which overrides the value configured in default model template.

9. For the GXV3275 used by the customer support supervisor, select an available extension for account 1 on "Basic" settings and click on "Save". Users can see the preview of the device configuration in "Advanced" settings. There is no model template configured for GXV3275.

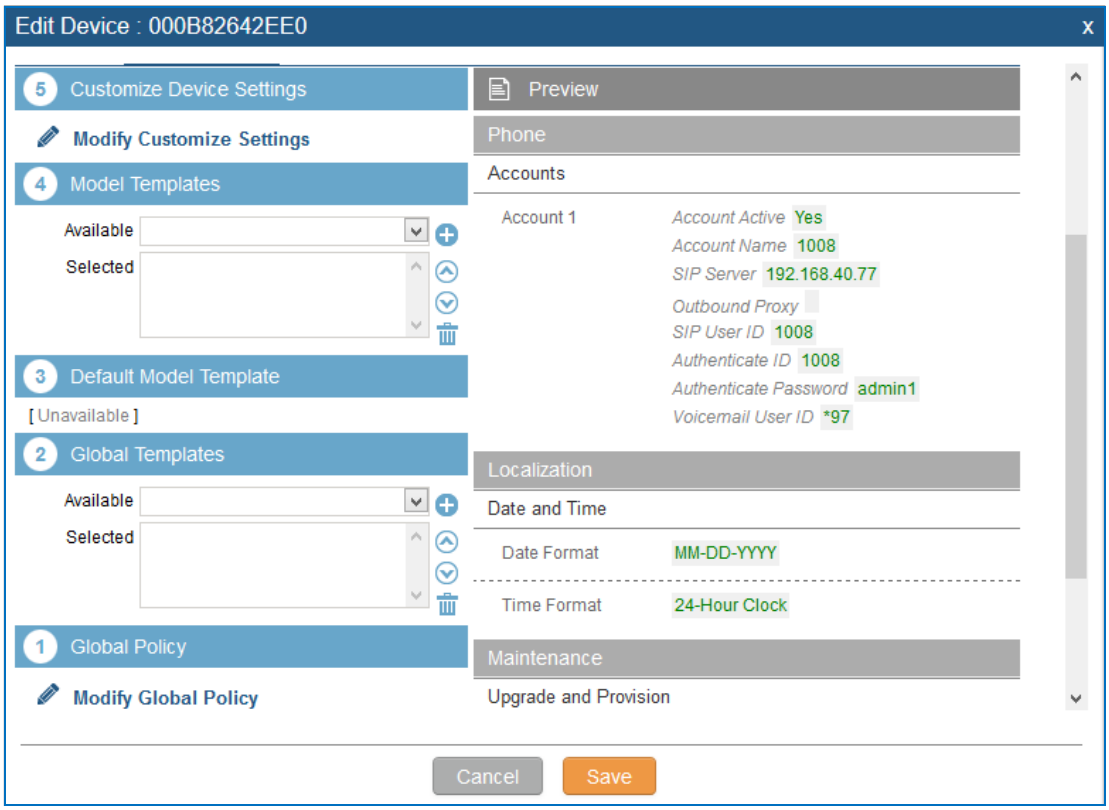


Figure 73: Zero Config Sample – Device Preview 3

10. Click on “Apply Changes” to apply saved changes.
11. On the web UI->**PBX**->**Zero Config**->**Zero Config** page, click on to send NOTIFY to trigger the device to download config file from UCM6510.

Now all the 9 phones in the network will be provisioned with an unique extension registered on the UCM6510. 3 of the phones will be provisioned to display Spanish on LCD and the other 5 will be provisioned to display English on LCD. The GXV3275 used by the supervisor will be provisioned to use the default language on LCD display since it’s not specified in the global policy.

EXTENSIONS

CREATE NEW USER

CREATE NEW SIP EXTENSION

To manually create new SIP user, go to web GUI->**PBX**->**Basic/Call Routes**->**Extensions**. Click on "Create New User"->"Create New SIP Extension" and a new dialog window will show for users to fill in the extension information. The configuration parameters are as follows.

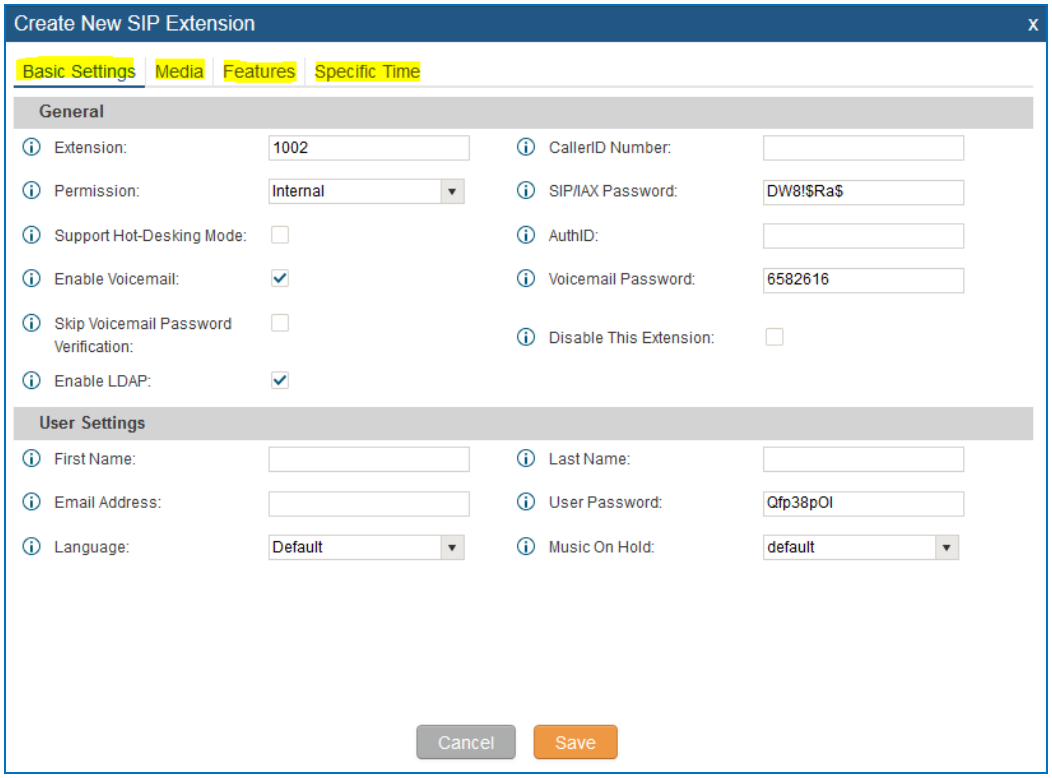


Figure 74: Create New Device

SIP extension options are divided into four categories:

- Basic Settings
- Media
- Features
- Specific Time

Click on the tag to view or edit options belonging to that category.
The configuration parameters are as follows.

Table 31: SIP Extension Configuration Parameters – Basic Settings

General	
Extension	The extension number associated with the user.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user. **Note:** The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Permission	Assign permission level to the user. The available permissions are “Internal”, “Local”, “National” and “International” from the lowest level to the highest level. The default setting is “Internal”. **Note:** Users need to have the same level as or higher level than an outbound rule’s privilege in order to make outbound calls using this rule.
SIP/IAX Password	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purpose.
Support Hot-Desking Mode	If enabled, SIP Password will accept only alphabet characters and digits; AuthID will be changed to the same as Extension.
Auth ID	Configure the authentication ID for the user. If not configured, the extension number will be used for authentication.
Enable Voicemail	Enable voicemail for the user. The default setting is “Yes”.
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the random generated password for security purpose.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.
Disable This Extension	If selected, this extension will be disabled on the UCM6510. **Note:** The disabled extension still exists on the PBX but can’t be used on the end device.
Enable LDAP	If enabled, this extension will be added to LDAP Phonebook PBX list; if disabled, this extension will be skipped when creating LDAP Phonebook.
User Settings	
First Name	Configure the first name of the user. The first name can contain

	characters, letters, digits and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User Password	Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
Language	Select the voice prompt language to be used for this extension. The default setting is "Default" which is the selected voice prompt language under web GUI->**PBX**->**Internal Options**->**Language**. The dropdown list shows all the current available voice prompt languages on the UCM6510. To add more languages in the list, please download voice prompt package by selecting "Check Prompt List" under web UI->**PBX**->**Internal Options**->**Language**.
Music On Hold	Select which Music On Hold class to suggest to extension when putting the active call on hold.

Table 32: SIP Extension Configuration Parameters – Media

SIP Settings	
NAT	Use NAT when the UCM6510 is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is one-way audio issue, usually it's related to NAT configuration or Firewall's support of SIP and RTP ports. The default setting is enabled.
Can Reinvite	By default, the UCM6510 will route the media steams from SIP endpoints through itself. If enabled, the PBX will attempt to negotiate with the endpoints to route the media stream directly. It is not always possible for the UCM6510 to negotiate endpoint-to-endpoint media routing. The default setting is "No".
DTMF Mode	Select DTMF mode for the user to send DTMF. The default setting is "RFC2833". If "Info" is selected, SIP INFO message will be used. If "Inband" is selected, 64-kbit PCMU and PCMA are required. When "Auto" is selected, RFC2833 will be used if offered, otherwise "Inband" will be used.
Insecure	• Port: Allow peers matching by IP address without matching port number. • Very: Allow peers matching by IP address without matching port number. Also, authentication of incoming INVITE messages is not required.

	• No: Normal IP-based peers matching and authentication of incoming INVITE. The default setting is “Port”.
Enable Keep-alive	If enabled, empty SDP packet will be sent to the SIP server periodically to keep the NAT port open. The default setting is “Yes”.
Keep-alive Frequency	Configure the Keep-alive interval (in seconds) to check if the host is up. The default setting is 60 seconds.
TEL URI	If the end device/phone has an assigned PSTN telephone number, this field should be set to “User=Phone”. Then a “User=Phone” parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to “Enable”, “Tel:” will be used instead of “SIP:” in the SIP request. The default setting is disabled.
SRTP	Enable SRTP for the call. The default setting is disabled.
Fax Mode	Select Fax mode. The default setting is “None”. • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->PBX->Internal Options->Fax/T.38.
Strategy	This option controls how the extension can be used on devices within different types of network. ・ Allow All Device in any network can register this extension. ・ Local Subnet Only Only the user in specific subnet can register this extension. Up to three subnet addresses can be specified. ・ A Specific IP Address Only the device on the specific IP address can register this extension. The default setting is “Allow All”.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G,726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263 and H.263p.

Table 33: SIP Extension Configuration Parameters – Features

Call Transfer	
Call Forward Unconditional	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The

	default setting is deactivated.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time condition are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”. Note: • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time condition are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”. Note: • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
CFB Time Condition	Select time condition for Call Forward Busy. The available time condition are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”. Note: • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.

CC Settings	
Enable CC	If enabled, UCM6510 will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason. By default it's disabled.
CC Mode	Two modes for Call Completion are supported: • **Normal**: This extension is used as ordinary extension. • **For Trunk**: This extension is registered from a PBX. The default setting is "Normal".
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel is allowed to make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.
External Number	Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of this time condition.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under web GUI->Internal Options->IVR Prompt: General Preference. The valid range is between 5 seconds and 600 seconds. Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under web GUI->CDR->Recording Files.
Skip Trunk Auth	· If set to 'yes', users can skip entering the password when making

	outbound calls. · If set to 'By Time', users can skip entering the password when making outbound calls during the selected time condition. · If set to 'No', users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If 'Skip Trunk Auth' is set to 'By Time', select a time condition during which users can skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.

Table 34: SIP Extension Configuration Parameters – Specific Time

Specific Time	
Time Condition	Click to add Time Condition to configure specific time for this extension.

CREATE NEW IAX EXTENSION

The UCM6510 supports Inter-Asterisk eXchange (IAX) protocol. IAX is used for transporting VoIP telephony sessions between servers and terminal devices. IAX is similar to SIP but also has its own characteristic. For more information, please refer to RFC5465.

To manually create new IAX user, go to web GUI->**PBX**->**Basic/Call Routes**->**Extensions**. Click on "Create New IAX Extension" and a new dialog window will show for users to fill in the extension information. The configuration parameters are as follows.

Table 35: IAX Extension Configuration Parameters – Basic Settings

General	
Extension	The extension number associated with the user.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user. **Note:** The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Permission	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". **Note:** Users need to have the same level as or higher level than an outbound rule's privilege in order to make outbound calls using this rule.

SIP/IAX Password	Configure the password for the user. A random secure password will be automatically generated. It is recommended to use this password for security purpose.
Enable Voicemail	Enable voicemail for the user. The default setting is “Yes”.
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the random generated password for security purpose.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.
Disable This Extension	If selected, this extension will be disabled on the UCM6510. **Note:** The disabled extension still exists on the PBX but can’t be used on the end device.
Enable LDAP	If enabled, this extension will be added to LDAP Phonebook PBX list; if disabled, this extension will be skipped when creating LDAP Phonebook.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits and _.
Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User Password	Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
Language	Select the voice prompt language to be used for this extension. The default setting is “Default” which is the selected voice prompt language under web GUI->**PBX**->**Internal Options**->**Language**. The dropdown list shows all the current available voice prompt languages on the UCM6510. To add more languages in the list, please download voice prompt package by selecting “Check Prompt List” under web UI->**PBX**->**Internal Options**->**Language**.
Music On Hold	Select which Music On Hold class to suggest to the extension when putting the active on hold.

Table 36: IAX Extension Configuration Parameters – Media

SIP Settings	
Max Number of Calls	Configure the maximum number of calls allowed for each remote IP address.
Require Call Token	Configure to enable/disable requiring call token. If set to “Auto”, it might lock out users who depend on backward compatibility when peer authentication credentials are shared between physical endpoints. The default setting is “Yes”.
SRTP	Enable SRTP for the call. The default setting is disabled.
Fax Mode	Select Fax Mode. The default setting is “None”. • None: Disable Fax. This is the default setting. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->PBX->Internal Options->Fax/T.38.
Strategy	This option controls how the extension can be used on devices within different types of network. • Allow All Device in any network can register this extension. • Local Subnet Only Only the user in specific subnet can register this extension. Up to three subnet addresses can be specified. • A Specific IP Address Only the device on the specific IP address can register this extension. The default setting is “Allow All”.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G,726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263 and H.263p.

Table 37: IAX Extension Configuration Parameters – Features

Call Transfer	
Call Forward Unconditional	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time condition are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”.

	Note: • "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.
CFN Time Condition	Select time condition for Call Forward No Answer. The available time condition are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Note: • "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
CFB Time Condition	Select time condition for Call Forward Busy. The available time condition are "Office Time", "Out of Office Time", "Holiday", "Out of Holiday", "Out of Office Time or Holiday" and "Specific". Note: • "Specific" has higher priority to "Office Times" if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.

External Number	Set the external number to be rang simultaneously. '-' is the connection character which will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of this time condition.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under web GUI->Internal Options->IVR Prompt: General Preference. The valid range is between 5 seconds and 600 seconds. Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under web GUI->CDR->Recording Files.
Skip Trunk Auth	• If set to "Yes", users can skip entering the password when making outbound calls. • If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition. • If set to "No", users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If "Skip Trunk Auth" is set to "By Time", select a time condition during which users can skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.

Table 38: IAX Extension Configuration Parameters – Specific Time

Specific Time	
Time Condition	Click to add Time Condition to configure specific time for this extension.

CREATE NEW FXS EXTENSION

The UCM6510 supports Foreign eXchange Subscriber (FXS) interface. FXS is used when user needs to connect analog phone lines or FAX machines to the UCM6510.

To manually create new FXS user, go to Web GUI->**PBX**->**Basic/Call Routes**->**Extensions**. Click on "Create New User"->"Create New FXS Extension" and a new dialog window will show for users to fill in the extension information. The configuration parameters are as follows.

Table 39: FXS Extension Configuration Parameters – Basic Settings

General	
Extension	The extension number associated with the user.
Analog Station	Select the FXS port to be assigned for this extension.
CallerID Number	Configure the CallerID Number that would be applied for outbound calls from this user. **Note:** The ability to manipulate your outbound Caller ID may be limited by your VoIP provider.
Permission	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". **Note:** Users need to have the same level as or higher level than an outbound rule's privilege in order to make outbound calls using this rule.
Enable Voicemail	Enable voicemail for the user. The default setting is "Yes".
Voicemail Password	Configure voicemail password (digits only) for the user to access the voicemail box. A random numeric password is automatically generated. It is recommended to use the random generated password for security purpose.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.
Disable This Extension	If selected, this extension will be disabled on the UCM6510. **Note:** The disabled extension still exists on the PBX but can't be used on the end device.
Enable LDAP	If enabled, this extension will be added to LDAP Phonebook PBX list; if disabled, this extension will be skipped when creating LDAP Phonebook.
User Settings	
First Name	Configure the first name of the user. The first name can contain characters, letters, digits and _.
Last Name	Configure the last name of the user. The last name can contain characters, letters, digits and _.

Email Address	Fill in the Email address for the user. Voicemail will be sent to this Email address.
User Password	Configure the password for user portal access. A random numeric password is automatically generated. It is recommended to use the randomly generated password for security purpose.
Language	Select the voice prompt language to be used for this extension. The default setting is "Default" which is the selected voice prompt language under web GUI->**PBX**->**Internal Options**->**Language**. The dropdown list shows all the current available voice prompt languages on the UCM6510. To add more languages in the list, please download voice prompt package by selecting "Check Prompt List" under web UI->**PBX**->**Internal Options**->**Language**.
Music On Hold	Select which Music On Hold class to suggest to extension when putting the active call on hold.

Table 40: FXS Extension Configuration Parameters – Media

Analog Settings	
Call Waiting	Configure to enable/disable call waiting feature. The default setting is "No".
User '#' as SEND	If configured, the # key can be used as SNED key after dialing the number on the analog phone. The default setting is "Yes".
RX Gain	Configure the RX gain for the receiving channel of analog FXS port. The valid range is -30Db to +6Db. The default setting is 0.
TX Gain	Configure the TX gain for the transmitting channel of analog FXS port. The valid range is -30Db to +6Db. The default setting is 0.
MIN RX Flash	Configure the minimum period of time (in milliseconds) that the hook-flash must remain unpressed for the PBX to consider the event as a valid flash event. The valid range is 30ms to 1000ms. The default setting is 200ms.
MAX RX Flash	Configure the maximum period of time (in milliseconds) that the hook-flash must remain unpressed for the PBX to consider the event as a valid flash event. The minimum period of time is 256ms and it can't be modified. The default setting is 1250ms.
Enable Polarity Reversal	If enabled, a polarity reversal will be marked as received when an outgoing call is answered by the remote party. For some countries, a polarity reversal is used for signaling the disconnection of a phone line and the call will be considered as hangup on a polarity reversal. The default setting is "Yes".
Echo Cancellation	Specify "ON", "OFF" or a value (the power of 2) from 32 to 1024 as the number of taps of cancellation.

	Note: When configuring the number of taps, the number 256 is not translated into 256ms of echo cancellation. Instead, 256 taps means 256/8 = 32 ms. The default setting is “ON”, which is 128 taps.
3-Way Calling	Configure to enable/disable 3-way calling feature on the user. The default setting is enabled.
Send CallerID After	Configure the number of rings before sending CID. Default setting is 1.
Fax Mode	For FXS extension, there are three options available in Fax Mode. The default setting is “None”. • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->PBX->Internal Options->Fax/T.38. • Fax Gateway: If selected, the UCM6510 can support conversation and processing of Fax data from T.30 to T.38 or T.38 to T.30. This feature is only available for FXS or FXO port.

Table 41: FXS Extension Configuration Parameters – Features

Call Transfer	
Call Forward Unconditional	Configure the Call Forward Unconditional target number. If not configured, the Call Forward Unconditional feature is deactivated. The default setting is deactivated.
CFU Time Condition	Select time condition for Call Forward Unconditional. CFU takes effect only during the selected time condition. The available time condition are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”. Note: • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.
Call Forward No Answer	Configure the Call Forward No Answer target number. If not configured, the Call Forward No Answer feature is deactivated. The default setting is deactivated.

CFN Time Condition	Select time condition for Call Forward No Answer. The available time condition are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”. Note: • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.
Call Forward Busy	Configure the Call Forward Busy target number. If not configured, the Call Forward Busy feature is deactivated. The default setting is deactivated.
CFB Time Condition	Select time condition for Call Forward Busy. The available time condition are “Office Time”, “Out of Office Time”, “Holiday”, “Out of Holiday”, “Out of Office Time or Holiday” and “Specific”. Note: • “Specific” has higher priority to “Office Times” if there is a conflict in terms of time period. • Specific time can be configured on the bottom of the extension configuration dialog. Scroll down the add Time Condition for specific time. • Office Time and Holiday could be configured on page Settings->Time Settings->Office Time/Holiday page.
CC Settings	
Enable CC	If enabled, UCM6510 will automatically alert this extension when a called party is available, given that a previous call to that party failed for some reason.
Ring Simultaneously	
Ring Simultaneously	Enable this option to have an external number ring simultaneously along with the extension. If a register trunk is used for outbound, the register number will be used to be displayed for the external number as caller ID number.
External Number	Set the external number to be rang simultaneously. ‘-’ is the connection character which will be ignored.
Time Condition for Ring Simultaneously	Ring the external number simultaneously along with the extension on the basis of this time condition.
Other Settings	
Ring Timeout	Configure the number of seconds to ring the user before the call is

	forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under web GUI->Internal Options->IVR Prompt: General Preference. The valid range is between 5 seconds and 600 seconds. Note: If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under web GUI->CDR->Recording Files.
Skip Trunk Auth	• If set to "Yes", users can skip entering the password when making outbound calls. • If set to "By Time", users can skip entering the password when making outbound calls during the selected time condition. • If set to "No", users will be asked to enter the password when making outbound calls.
Time Condition for Skip Trunk Auth	If "Skip Trunk Auth" is set to "By Time", select a time condition during which users can skip entering password when making outbound calls.
Dial Trunk Password	Configure personal password when making outbound calls via trunk.

Table 42: FXS Extension Configuration Parameters – Specific Time

Specific Time	
Time Condition	Click to add Time Condition to configure specific time for this extension.

BATCH ADD EXTENSIONS

BATCH ADD SIP EXTENSIONS

In order to add multiple SIP extensions, BATCH add can be used to create standardized SIP extension accounts. However, unique extension user name can't be set using BATCH add.

Under web GUI->**PBX**->**Basic/Call Routes**->**Extensions**, click on "Batch Add Extensions"->"Batch Add SIP Extensions".

Table 43: Batch Add SIP Extension Parameters

General	
Start Extension	Configure the starting extension number of the batch of extensions to be added.

Create Number	Specify the number of extensions to be added. The default setting is 5.
Permission	Assign permission level to the user. The available permissions are “Internal”, “Local”, “National” and “International” from the lowest level to the highest level. The default setting is “Internal”. **Note:** Users need to have the same level as or higher level than an outbound rule’s privilege in order to make outbound calls using this rule. If the outbound rule privilege is disabled, this option will not take effect.
Enable Voicemail	Enable Voicemail for the user. The default setting is “Yes”.
SIP/IAX Password	Configure the SIP/IAX password for the users. Two options are available to create password for the batch of extensions. • User Random Password. A random secure password will be automatically generated. It is recommended to use this password for security purpose. • Enter a password to be used on all the extensions in the batch.
Voicemail Password	Configure Voicemail password (digits only) for the users. • User Random Password. A random password in digits will be automatically generated. It is recommended to use this password for security purpose. • Enter a password to be used on all the extensions in the batch.
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under web GUI->**Internal Options**: General Preference. The valid range is between 5 seconds and 600 seconds. **Note:** If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files will be saved in external storage if plugged in and can be accessed under web GUI->**CDR**->**Recording Files**.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.
Music On Hold	Select which Music On Hold class to suggest to extensions when putting them on hold.

Enable LDAP	If enabled, the batch added extensions will be added to LDAP Phonebook PBX list; if disabled, the batch added extensions will be skipped when creating LDAP Phonebook.
SIP Settings	
NAT	Use NAT when the PBX is on a public IP communicating with devices hidden behind NAT (e.g., broadband router). If there is one-way audio issue, usually it's related to NAT configuration or Firewall's support of SIP and RTP ports. The default setting is enabled.
Can Reinvite	By default, the PBX will route the media steams from SIP endpoints through itself. If enabled, the PBX will attempt to negotiate with the endpoints to route the media stream directly. It is not always possible for the PBX to negotiate endpoint-to-endpoint media routing. The default setting is "No".
DTMF Mode	Select DTMF mode for the user to send DTMF. The default setting is "RFC2833". If "Info" is selected, SIP INFO message will be used. If "Inband" is selected, 64-kbit codec PCMU and PCMA are required. When "Auto" is selected, RFC2833 will be used if offered, otherwise "Inband" will be used.
Insecure	• Port: Allow peers matching by IP address without matching port number. • Very: Allow peers matching by IP address without matching port number. Also, authentication of incoming INVITE messages is not required. • No: Normal IP-based peers matching and authentication of incoming INVITE. The default setting is "Port".
Enable Keep-alive	If enabled, empty SDP packet will be sent to the SIP server periodically to keep the NAT port open. The default setting is "Yes".
Keep-alive Frequency	Configure the number of seconds for the host to be up for Keep-alive. The default setting is 60 seconds.
TEL URI	If the end device/phone has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
Other Settings	
SRTP	Enable SRTP for the call. The default setting is "No".
Fax Mode	Select Fax mode for this user. The default setting is "None".

	• None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->PBX->Internal Options->Fax/T.38. **Note:** If enabled, Fax Pass-through cannot be used.
Strategy	This option controls how the extension can be used on devices within different types of network. • Allow All Device in any network can register this extension. • Local Subnet Only Only the user in specific subnet can register this extension. Up to three subnet addresses can be specified. • A Specific IP Address. Only the device on the specific IP address can register this extension. The default setting is "Allow All".
Skip Trunk Auth	If enabled, users will not need enter the "PIN Set" required by the outbound rule to make outbound calls. The default setting is "No".
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.722, G.729, G.723, ILBC, ADPCM, LPC10, H.264, H.263 and H.263p. In the selected codec list, users can click on UP or DOWN arrow to adjust the order for the codec priority.

BATCH ADD IAX EXTENSIONS

Under Web GUI->**PBX**->**Basic/Call Routes**->**Extensions**, click on "Batch Add Extensions"->"Batch Add IAX Extensions".

Table 44: Batch Add IAX Extension Parameters

General	
Start Extension	Configure the starting extension number of the batch of extensions to be added.
Create Number	Specify the number of extensions to be added. The default setting is 5.
Permission	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".

	Note: Users need to have the same level as or higher level than an outbound rule's privilege in order to make outbound calls from this rule.
Enable Voicemail	Enable Voicemail for the user. The default setting is "Yes".
SIP/IAX Password	Configure the SIP/IAX password for the users. Three options are available to create password for the batch of extensions. • User Random Password. A random secure password will be automatically generated. It is recommended to use this password for security purpose. • Use Extension as Password. • Enter a password to be used on all the extensions in the batch.
Voicemail Password	Configure Voicemail password (digits only) for the users. • User Random Password. A random password in digits will be automatically generated. It is recommended to use this password for security purpose. • Use Extension as Password. • Enter a password to be used on all the extensions in the batch.
Ring Timeout	Configure the number of seconds to ring the user before the call is forwarded to voicemail (voicemail is enabled) or hang up (voicemail is disabled). If not specified, the default ring timeout is 60 seconds on the UCM6510, which can be configured in the global ring timeout setting under web GUI->**Internal Options**->**IVR Prompt**: General Preference. The valid range is between 5 seconds and 600 seconds. **Note:** If the end point also has a ring timeout configured, the actual ring timeout used is the shortest time set by either device.
Auto Record	Enable automatic recording for the calls using this extension. The default setting is disabled. The recording files can be accessed under web GUI->**CDR**->**Recording Files**.
Skip Voicemail Password Verification	When user dials voicemail code, the password verification IVR is skipped. If enabled, this would allow one-button voicemail access. By default this option is disabled.
Music On Hold	Select which Music On Hold class to suggest to extensions when putting them on hold.
Enable LDAP	If enabled, the batch added extensions will be added to LDAP Phonebook PBX list; if disabled, the batch added extensions will be skipped when creating LDAP Phonebook.
IAX Settings	
Max Number of Calls	Configure the maximum number of calls allowed for each remote IP

	address.
Require Call Token	Configure to enable/disable requiring call token. If set to “Auto”, it might lock out users who depend on backward compatibility when peer authentication credentials are shared between physical endpoints. The default setting is “Yes”.
Other Settings	
SRTP	Enable SRTP for the call. The default setting is “No”.
Fax Mode	Select Fax Mode for this user. The default setting is “None”. • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->**PBX**->**Internal Options**->**Fax/T.38**.
Strategy	This option controls how the extension can be used on devices within different types of network. ・ Allow All Device in any network can register this extension. ・ Local Subnet Only Only the user in specific subnet can register this extension. Up to three subnet addresses can be specified. ・ A Specific IP Address. Only the device on the specific IP address can register this extension. The default setting is “Allow All”.
Skip Trunk Auth	If enable “All”, users do not need to enter password when making an outbound call. If enable “Follow Me”, the call can dial out via follow me without password.
Codec Preference	Select audio and video codec for the extension. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.722, G.729, G.723, ILBC, ADPCM, LPC10, H.264, H.263 and H.263p.

SEARCH AND EDIT EXTENSION

All the UCM6510 extensions are listed under web GUI->**PBX**->**Basic/Call Routes**->**Extensions**, with status, Extension, CallerID Name, Technology (SIP, IAX and FXS), IP and Port. Each extension has a checkbox for users to “Modify Selected Extensions” or “Delete Selected Extensions”. Also, options “Edit” , “Reboot” and “Delete” are available per extension. User can search an extension by specifying the extension number to find an extension quickly.

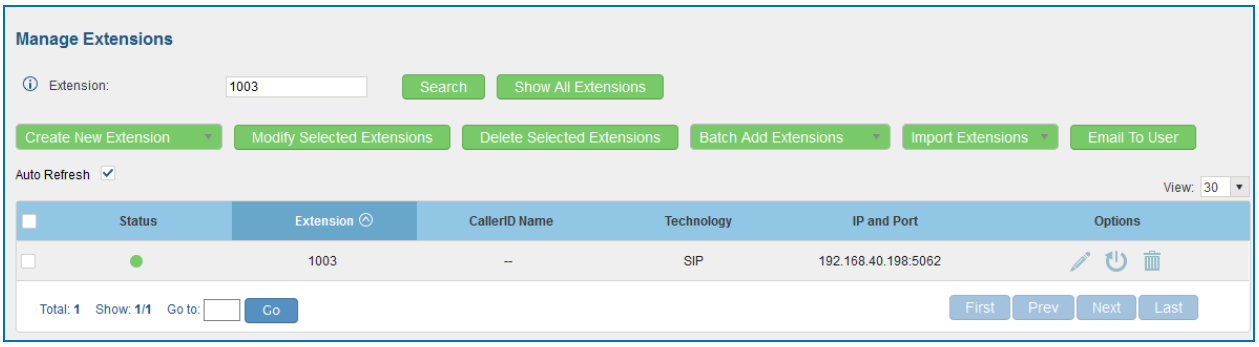


Figure 75: Manage Extensions

- **Status**
  Users can see the following icon for each extension to indicate the SIP status.

  Green: Free
  Blue: Ringing
  Yellow: In Use
  Grey: Unavailable

- **Edit single extension**

  Click on to start editing the extension parameters.

- **Reboot the user**

  Click on to send NOTIFY reboot event to the device which has an UCM6510 extension already registered. To successfully reboot the user, “Zero Config” needs to be enabled on the UCM6510 web GUI->**PBX**->**Basic/Call Routes**->**Zero Config**->**Auto Provisioning Settings**.

- **Delete single extension**

  Click on to delete the extension. Or select the checkbox of the extension and then click on “Delete Selected Extensions”.

- **Modify selected extensions**
  Select the checkbox for the extension(s). Then click on “Modify Selected Extensions” to edit the extensions in a batch.

- **Delete selected extensions**
  Select the checkbox for the extension(s). Then click on “Delete Selected Extensions” to delete the extension(s).

EXPORT EXTENSIONS

The extensions configured on the UCM6510 can be exported to csv format file with selected technology "SIP", "IAX" or "FXS". Click on "Import Extensions" scroll down to select "Export Extensions" button and select technology in the prompt.

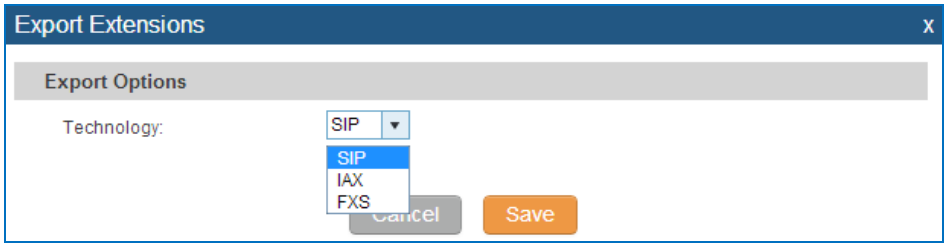


Figure 76: Export Extensions

The exported csv file can also serve as a template for users to fill in desired extension information to be imported to the UCM6510.

IMPORT EXTENSIONS

The capability to import extensions to the UCM6510 provides users flexibility to batch add extensions with similar or different configurations quickly.

1. Export extension csv file from the UCM6510 by clicking on "Export Extensions" button.
2. Fill up the extension information you would like in the exported csv template.
3. Click on "Import Extensions" button. The following dialog will be prompted.

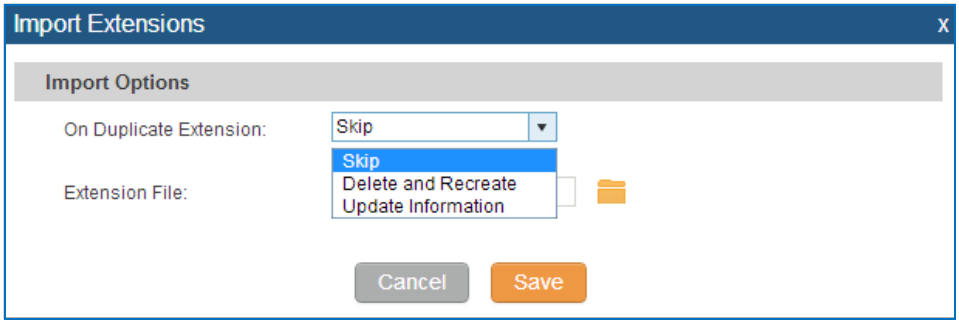


Figure 77: Export Extensions

4. Select the option in "On Duplicate Extension" to define how the duplicate extension(s) in the imported csv file should be treated by the PBX.

- Skip: Duplicate extensions in the csv file will be skipped. The PBX will keep the current extension information as previously configured without change.
- Delete and Recreate: The current extension previously configured will be deleted and the duplicate extension in the csv file will be loaded to the PBX.
- Update Information: The current extension previously configured in the PBX will be kept. However, if the duplicate extension in the csv file has different configuration for any options, it will override the configuration for those options in the extension.

5. Click on to select csv file from local directory in the PC for uploading.
6. Click on "Save" to import the csv file.
7. Click on "Apply Changes" to apply the imported file on the UCM6510.

EMAIL TO USER

Once the extensions are created with Email address, the PBX administrator can click on button "Email To User" to send the account registration and configuration information to the user. Please make sure Email setting under web UI->**Settings**->**Email Settings** is properly configured and tested on the UCM6510 before using "Email To User".

When click on "Email To User" button, the following message will be prompted in the web page. Click on OK to confirm sending the account information to all users' Email addresses.

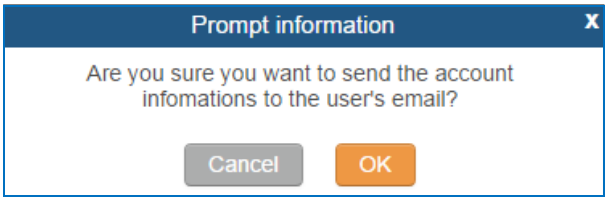


Figure 78: Email To User: Prompt Information

The user will receive Email including account registration information and LDAP configuration. A QR code is also generated for Mobile applications to scan it and get automatically provisioned. QR code provisioning is supported on Grandstream Softphone GS Wave Android™ application.

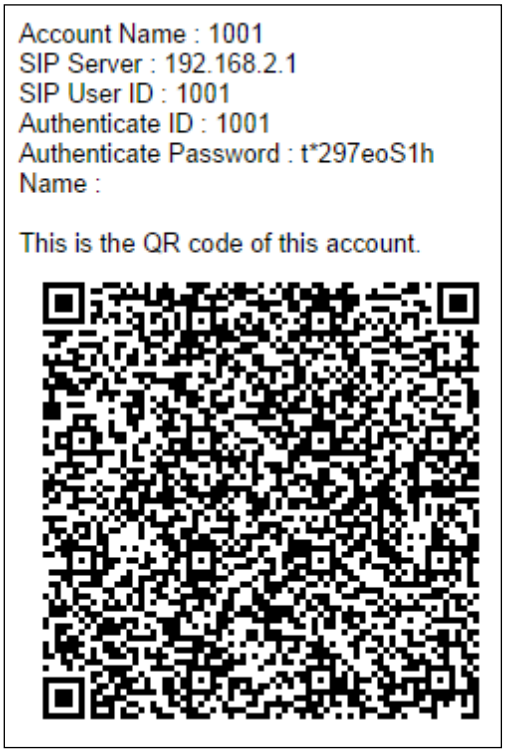

Account Name : 1001
SIP Server : 192.168.2.1
SIP User ID : 1001
Authenticate ID : 1001
Authenticate Password : t*297eoS1h
Name :
This is the QR code of this account.

Figure 79: Email To User: Account Registration Information and QR Code

Figure 80: Email To User: LDAP Client Information and QR Code

This page intentionally left blank

ANALOG TRUNKS

To set up analog trunk on the UCM6510:

- Go to web GUI->**PBX**->**Basic/Call Routes**->**Analog Trunks** to add and edit analog trunks.
- Go to web GUI->**PBX**->**Ports Config**->**Analog Hardware** to configure analog hardware settings.

ANALOG TRUNKS CONFIGURATION

Go to web GUI->**PBX**->**Basic/Call Routes**->**Analog Trunks** to add and edit analog trunks.

- Click on “Create New Analog Trunk” to add a new analog trunk.
- Click on to edit the analog trunk.
- Click on to delete the analog trunk.

The analog trunk options are listed in the table below.

Table 45: Analog Trunk Configuration Parameters

Channels	Select the channel for the analog trunk.
Trunk Name	Specify a unique label to identify the trunk when listed in outbound routes, inbound routes and etc.
SLA Mode	Enable this option to satisfy two primary use cases, which include emulating a simple key system and creating shared extensions on a PBX. Enable SLA Mode will disable polarity reversal.
Barge Allowed	The barge option specifies whether or not other stations are allowed to join a call in progress on this trunk. If enabled, the other stations can press the line button to join the call. The default setting is Yes.
Hold Access	The hold option specifies hold permissions for this trunk. If set to “Open”, any station can place this trunk on hold and any other station is allowed to retrieve the call. If set to “Private”, only the station that places the call on hold can retrieve the call. The default setting is Yes.
Advanced Options	
Enable Polarity Reversal	If enabled, a polarity reversal will be marked as received when an outgoing call is answered by the remote party. For some countries, a polarity reversal is used for signaling the disconnection of a phone line and the call

	will be considered as “hangup” on a polarity reversal. The default setting is “No”.
Polarity on Answer Delay	When FXO port answers the call, FXS may send a Polarity Reversal. If this interval is shorter than the value of “Polarity on Answer Delay”, the Polarity Reversal will be ignored. Otherwise, the FXO will onhook to disconnect the call. The default setting is 600ms.
Current Disconnect Threshold (ms)	This is the periodic time (in ms) that the UCM6510 will use to check on a voltage drop in the line. The default setting is 200. The valid range is 50 to 3000.
Ring Timeout	Configure the ring timeout (in ms). Trunk (FXO) devices must have a timeout to determine if there was a hangup before the line is answered. This value can be used to configure how long it takes before the UCM6510 considers a non-ringing line with hangup activity. The default setting is 8000.
RX Gain	Configure the RX gain for the receiving channel of analog FXO port. The valid range is from -13.5 (Db) to + 12.0 (Db). The default setting is 0.
TX Gain	Configure the TX gain for the transmitting channel of analog FXO port. The valid range is from -13.5 (Db) to + 12.0 (Db). The default setting is 0.
Use CallerID	Configure to enable CallerID detection. The default setting is “Yes”.
Fax Detection	Enable to detect Fax signal from the trunk during the call and send the received Fax to the default Email address in Fax setting page under web GUI->PBX->Internal Options->Fax/T.38. The default setting is “No”. **Note:** If enabled, Fax Pass-through cannot be used.
Caller ID Scheme	Select the Caller ID scheme for this trunk. If you are not sure which scheme to choose, please select “Auto Detect”. The default setting is “Bellcore/Telcordia”.
FXO Dial Delay(ms)	Configure the time interval between off-hook and first dialed digit for outbound calls.
Auto Record	Enable automatic recording for the calls using this trunk. The default setting is disabled. The recording files are saved in external storage device if plugged in and can be accessed under web GUI->**CDR**->**Recording Files**.
Disable This Trunk	If selected, the trunk will be disabled.
DAHDI Out Line Selection	This is to implement analog trunk outbound line selection strategy. Three options are available: • Ascend When the call goes out from this analog trunk, it will always try to use

	the first idle FXO port. The port order that the call will use to go out would be port 1->port 2->port 10->port 16. Every time it will start with port 1 (if it's idle). • Poll When the call goes out from this analog trunk, it will use the port that is not used last time. And it will always use the port in the order of port 1->2->10->16->1->2->10->16->1->2->10->16…, following the last port being used. • Descend When the call goes out from this analog trunk, it will always try to use the last idle FXO port. The port order that the call will use to go out would be port 16->port 10->port 2->port 1. Every time it will start with port 16 (if it's idle). The default setting is "Ascend" mode.
Tone Settings	
Busy Detection	Busy Detection is used to detect far end hangup or for detecting busy signal. The default setting is "Yes".
Busy Tone Count	If "Busy Detection" is enabled, users can specify the number of busy tones to be played before hanging up. The default setting is 2. Better results might be achieved if set to 4, 6 or even 8. Please note that the higher the number is, the more time is needed to hangup the channel. However, this might lower the probability to get random hangup.
Congestion Detection	Congestion detection is used to detect far end congestion signal. The default setting is "Yes".
Congestion Count	If "Congestion Detection" is enabled, users can specify the number of congestion tones to wait for. The default setting is 2.
Tone Country	Select the country for tone settings. If "Custom" is selected, users could manually configure the values for Busy Tone and Congestion Tone. The default setting is "United States of America (USA)".
Busy Tone	Syntax: f1=val[@level][,f2=val[@level]],c=on1/off1[-on2/off2[-on3/off3]]; Frequencies are in Hz and cadence on and off are in ms. Frequencies Range: [0, 4000] Busy Level Range: (-300, 0) Cadence Range: [0, 16383]. Select Tone Country "Custom" to manually configure Busy Tone value. Default value: f1=480@-50,f2=620@-50,c=500/500

Congestion Tone	Syntax: f1=val[@level][,f2=val[@level]],c=on1/off1[-on2/off2[-on3/off3]]; Frequencies are in Hz and cadence on and off are in ms. Frequencies Range: [0, 4000] Busy Level Range: (-300, 0) Cadence Range: [0, 16383]. Select Tone Country "Custom" to manually configure Busy Tone value. Default value: f1=480@-50,f2=620@-50,c=250/250
PSTN Detection	Click on "Detect" to detect the busy tone, Polarity Reversal and Current Disconnect by PSTN. Before the detecting, please make sure there are more than one channel configured and working properly. If the detection has busy tone, the "Tone Country" option will be set as "Custom".

PSTN DETECTION

The UCM6510 provides PSTN detection function to help users detect the busy tone, Polarity Reversal and Current Disconnect by making a call from the PSTN line to another destination. The detecting call will be answered and up for about 1 minute. Once done, the detecting result will show and can be used for the UCM6510 settings.

1. Go to UCM6510 web GUI->**PBX**->**Basic/Call Routes**->**Analog Trunks** page.
2. Click to edit the analog trunk created for the FXO port.
3. In the dialog window to edit the analog trunk, go to "Tone Settings" section and click on Detect for "PSTN Detection".

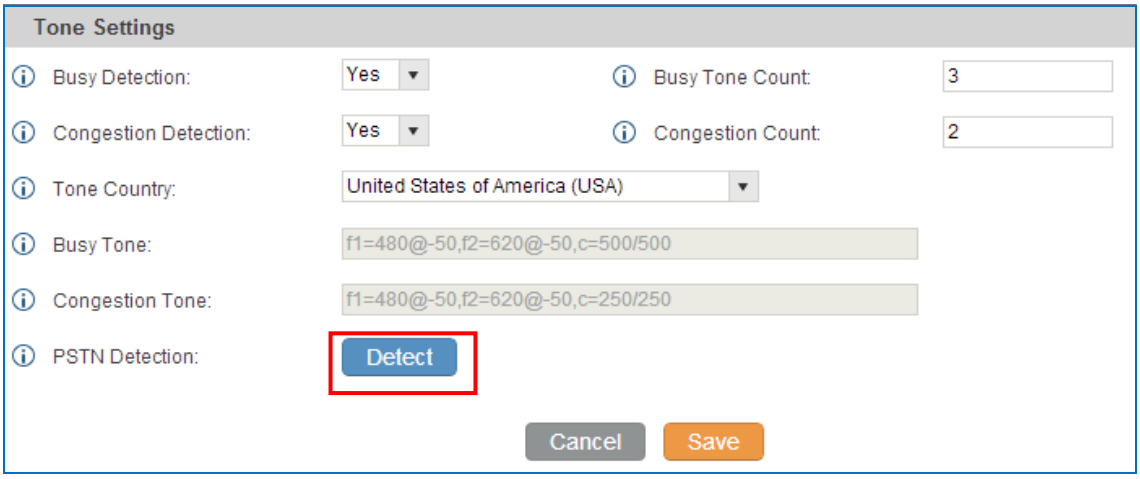


Figure 81: UCM6510 FXO Tone Settings

4. Click on “Detect” to start PSTN detection.

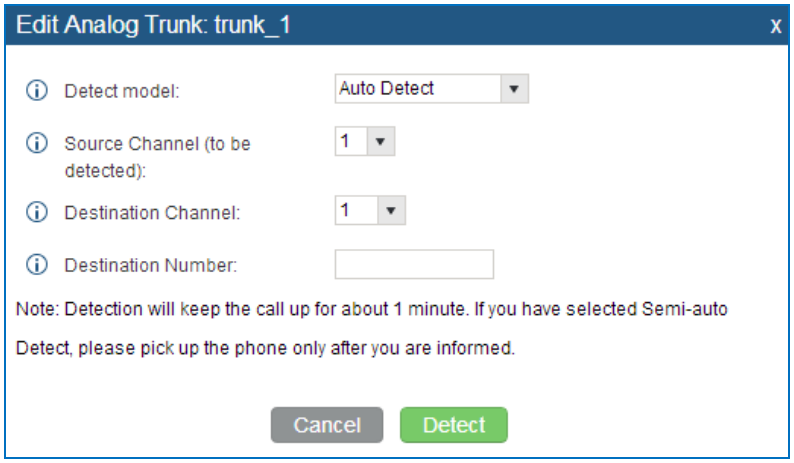

Edit Analog Trunk: trunk_1
x
Detect model:
Auto Detect
Source Channel (to be detected):
1
Destination Channel:
1
Destination Number:
Note: Detection will keep the call up for about 1 minute. If you have selected Semi-auto Detect, please pick up the phone only after you are informed.
Cancel
Detect

Figure 82: UCM6510 PSTN Detection

- If there are two FXO ports connected to PSTN lines, use the following settings for auto-detection.

  Detect Model: Auto Detect.
  Source Channel: The source channel to be detected.
  Destination Channel: The channel to help detecting. For example, the second FXO port.
  Destination Number: The number to be dialed for detecting. This number must be the actual PSTN number for the FXO port used as the destination channel.

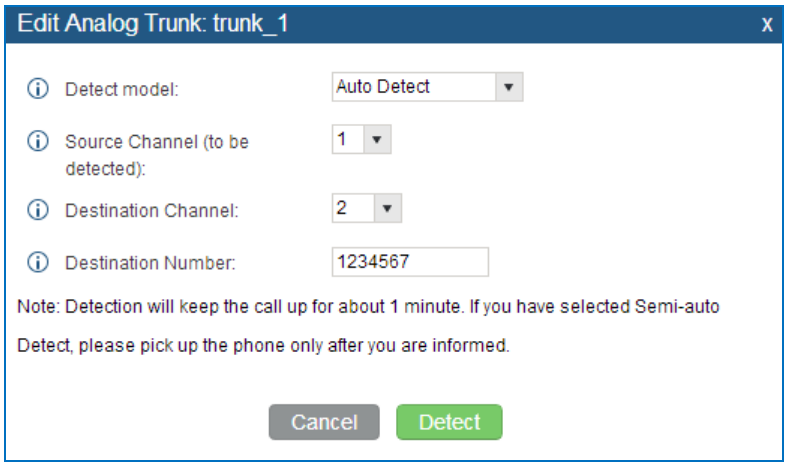


Figure 83: UCM6510 PSTN Detection: Auto Detect

- If there is only one FXO port connected to PSTN line, use the following settings for auto-detection.

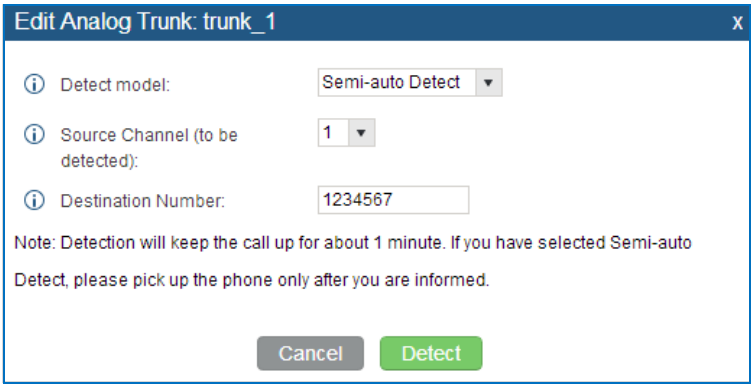

Edit Analog Trunk: trunk_1
x
Detect model:
Semi-auto Detect
Source Channel (to be detected):
1
Destination Number:
1234567
Note: Detection will keep the call up for about 1 minute. If you have selected Semi-auto Detect, please pick up the phone only after you are informed.
Cancel
Detect

Figure 84: UCM6510 PSTN Detection: Semi-Auto Detect

Detect Model: Semi-auto Detect.
Source Channel: The source channel to be detected.
Destination Number: The number to be dialed for detecting. This number could be a cell phone number or other PSTN number that can be reached from the source channel PSTN number.

5. Click “Detect” to start detecting. The source channel will initiate a call to the destination number. For “Auto Detect”, the call will be automatically answered. For “Semi-auto Detect”, the UCM6510 web GUI will display prompt to notify the user to answer or hang up the call to finish the detecting process.

6. Once done, the detected result will show. Users could save the detecting result as the current UCM6510 settings.

Table 46: PSTN Detection for Analog Trunk

Detect Model	Select “Auto Detect” or “Semi-auto Detect” for PSTN detection. • Auto Detect Please make sure two or more channels are connected to the UCM6510 and in idle status before starting the detection. During the detection, one channel will be used as caller (Source Channel) and another channel will be used as callee (Destination Channel). The UCM6510 will control the call to be established and hang up between caller and callee to finish the detection. • Semi-auto Detect Semi-auto detection requires answering or hanging up the call manually. Please make sure one channel is connected to the UCM6510 and in idle status before starting the detection. During the detection, source channel will be used as caller and send the call to the configured Destination Number. Users will then need follow the prompts in web GUI to help finish the detection.

	The default setting is “Auto Detect”.
Source Channel	Select the channel to be detected.
Destination Channel	Select the channel to help detect when “Auto Detect” is used.
Destination Number	Configure the number to be called to help the detection.

⚠ **Note:**

- The PSTN detection process will keep the call up for about 1 minute.
- If “Semi-auto Detect’ is used, please pick up the call only after informed from the web GUI prompt.
- Once the detection is successful, the detected parameters “Busy Tone”, “Polarity Reversal” and “Current Disconnect by PSTN” will be filled into the corresponding fields in the analog trunk configuration.

ANALOG HARDWARE CONFIGURATION

The analog hardware (FXS port and FXO port) on the UCM6510 can be configured under web GUI->**PBX**->**Ports Config**->**Analog Hardware**. Click on to edit signaling preference for FXS port or configure ACIM settings for FXO port.

Select “Loop Start” or “Kewl Start” for each FXS port. And then click on “Update” to save the change.

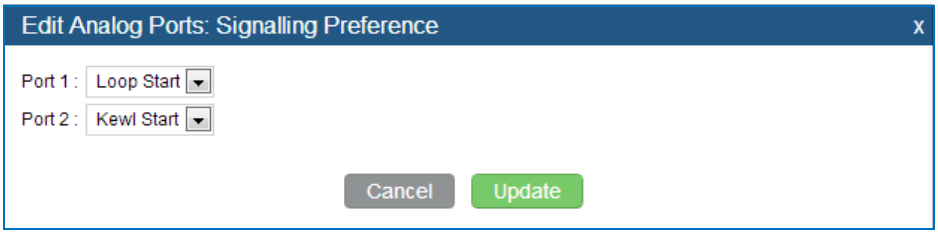


Figure 85: FXS Ports Signaling Preference

For FXO port, users could manually enter the ACIM settings by selecting the value from dropdown list for each port. Or users could click on “Detect” for the UCM6510 to automatically detect the ACIM value. The detecting value will be automatically filled into the settings.

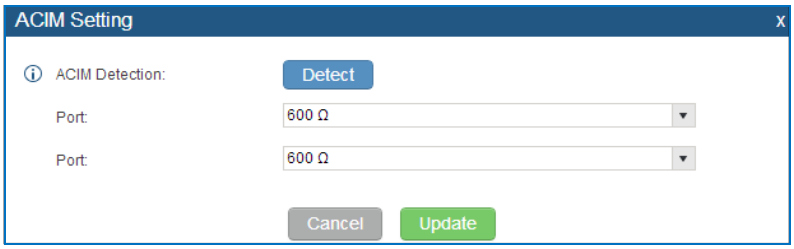


Figure 86: FXO Ports ACIM Settings

Note:

ACIM setting is very important for the FXO/PSTN line to work properly on the UCM6510. If the users experience echo, caller ID or disconnecting issue, please make sure to run the ACIM detection to find out the correct value for impedance setting.

Table 47: Analog Hardware Configuration Parameters

Tone Region	Select country to set the default tones for dial tone, busy tone, ring tone and etc to be sent from the FXS port. The default setting is “United States of America (USA)”.
Advanced Settings	
FXO Opermode	Select country to set the On Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country’s analog line characteristics. The default setting is “United States of America (USA)”.
FXS Opermode	Select country to set the On Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage adjustment, Minimum Operational Loop Current, and AC Impedance as predefined for your country’s analog line characteristics. The default setting is “United States of America (USA)”.
FXS TISS Override	Configure to enable or disable override Two-Wire Impedance Synthesis (TISS). The default setting is No. If enabled, users can select the impedance value for Two-Wire Impedance Synthesis (TISS) override. The default setting is 600Ω.
PCMA Override	Select the codec to be used for analog lines. North American users should

	choose PCMU. All other countries, unless already known, should be assumed to be PCMA. The default setting is PCMU. **Note:** This option requires system reboot to take effect.
Boost Ringer	Configure whether normal ringing voltage (40V) or maximum ringing voltage (89V) for analog phones attached to the FXS port is required. The default setting is “Normal”.
Fast Ringer	Configure to increase the ringing speed to 25HZ. This option can be used with “Low Power” option. The default setting is “Normal”.
Low Power	Configure the peak voltage up to 50V during “Fast Ringer” operation. This option is used with “Fast Ringer”. The default setting is “Normal”.
Ring Detect	If set to “Full Wave”, false ring detection will be prevented for lines where Caller ID is sent before the first ring and proceeded by a polarity reversal, as in UK. The default setting is “Standard”.
FXS MWI Mode	Configure the type of Message Waiting Indicator on FXS lines. The default setting is “FSK”. • FSK: Frequency Shift Key Indicator • NEON: Light Neon Bulb Indicator.

This page intentionally left blank

DIGITAL TRUNKS

The UCM6510 supports E1/T1/J1 which are physical connection technology used in digital network. T1 is the North American standard, J1 is used in Japan, whereas E1 is the European standard.

UCM6510 supports four signaling protocols: PRI, MFC/R2, SS7, E&M Immediate and E&M Wink. PRI provides a varying number of channels depending on the standards in the country of implementation (E1, T1 or J1); MFC/R2 is a signaling protocol heavily used over E1 trunks; SS7 uses out-of-band signaling, which travels on a separate, dedicated channel rather than within the same channel as the telephone call, providing more efficiency and higher security level when the telephone calls are set up. E&M Immediate and E&M Wink are only valid when using T1 port.

To set up digital trunk on the UCM6510:

1. Go to web UI->**PBX**->**Ports Config**->**Digital Hardware** to configure port type and channels.
2. Go to web UI->**PBX**->**Basic/Call Routes**->**Digital Trunks** to add and edit digit trunk.
3. Go to web UI->**PBX**->**Basic/Call Routes**->**Outbound Routes** and **Inbound Routes** to configure outbound and inbound rule for the digital trunk.

DIGITAL HARDWARE CONFIGURATION

Go to web GUI->**PBX**->**Ports Config**->**Digital Hardware** page and configure the following:

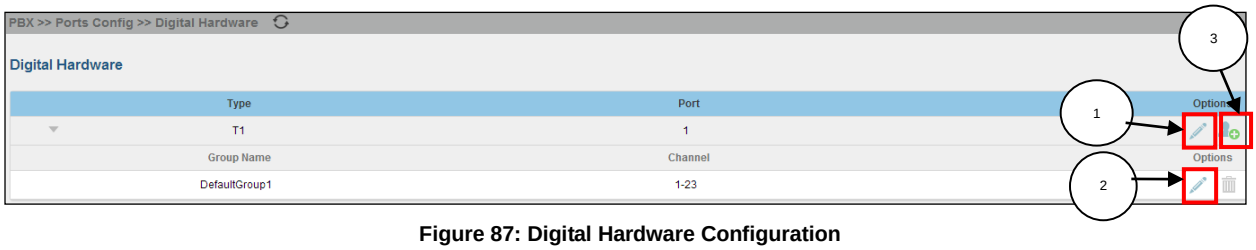


Figure 87: Digital Hardware Configuration

- **Step 1**: Click on to edit digital ports. Please see configuration parameters in the tables below.
- **Step 2**: Click on to edit group. This assigns channels to be used for the digital port. For E1, 30 B channels can be assigned to the default group; for T1/J1, 23 B channels can be assigned to the default group.
- **Step 3**: If fewer than 30 B channels for E1 or 23 B channels for T1/J1 are assigned in default group, users can click on to add more groups. This is not necessary in most cases and only default

group is needed.

⚠ **Note:**

Currently, the group configuration in digit trunks settings is to manage outbound routes only. It doesn't control inbound routes. Therefore, if the users have configured multiple groups for the digital trunk, please make sure the inbound routes for those groups have the same inbound rule configured. Otherwise, inbound call using the digital trunk might not work properly.

The UCM6510 currently supports E1, T1 and J1 digital hardware type. When different signaling is selected for E1, T1 or J1, the settings in basic options and advanced options will be different. The following tables list all the settings to configure digital ports when selecting each signaling.

Table 48: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE

Basic Settings	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it. • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1/J1 link is the preferred source of the master clock.
LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0Db unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24Db to +12Db.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24Db to +12Db.
Codec	Select alaw or ulaw. If set to default, alaw will be used for E1.
Play Local RBT	This configured whether to play the ringback tone from local UCM6510 or not. If enabled, the local UCM6510 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default

	setting is disabled.
Advanced Settings	
Switch Type	Select switch type. • EuroISDN: EuroISDN (common in Europe) • NI2: National ISDN type 2 (common in the US) • DMS100: Nortel DMS100 • 4ESS: AT&T 4ESS • 5ESS: Lucent 5ESS • NI1: old national ISDN type 1 • Q.SIG
Coding	Select “HDB3” or “AMI”.
CRC	Select whether to use CRC4 or not.
PRI Dial Plan	This setting is used to specify the type of the callee number. The service provider will usually verify this. The default setting is “unknown”. In some very unusual circumstances, you may need set to “Dynamic” or “Redundant”. **Note:** When one type is selected, you might not be able to dial another class of numbers. For example, if “National” is configured, you won’t be able to dial local or international numbers.
PRI Local Dial Plan	This setting is used to specify the type of the caller number. The service provider will usually verify this.
D-Chan	Indicates the D channel for control.
International Prefix National Prefix Local Prefix Private Prefix Unknown Prefix	Configure the prefix in PRI Local Dial Plan and PRI Dial Plan for each type.
PRI T310	Configure PRI T310 Timer (in seconds). The default value is 10 seconds.
PRI Indication	Select the PRI Indication. • outofband: Use RELEASE, DISCONNECT or other messages with CAUSE to indicate call progress (e.g., cause: unassigned number or user busy). • inband: use in-band tones to play busy or congestion signal to the other side. This is the default setting.
Reset Interval	The interval that restarts idle channels.
PRI Exclusive	This setting is used to set up the ChannelID in SETUP message. If enabled, only the specified B channel can be used. Otherwise, select one

	of the channels in B channel. If you need override the existing channels selection routine and force all PRI channels to be marked as exclusively selected, please enable it.
Facility Enable	If selected, transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility) will be enabled.
NSF	Some switches (AT&T especially) require network specific facility. Currently the supported values are "none", "sdn", "megacom", "tollfreemegacom", "accunet".

Table 49: Digital Hardware Configuration Parameters: E1 - SS7

Basic Settings	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it. • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.
SS7 Variant	Select ITU, ANSI or CHINA.
Originating Point Code	Originating point code is used to identify the node originating the message, always provided by the operator/ISP. • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
Destination Point Code	Destination point code is the address to send the message to, always be provided by the operator/ISP. • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
First CIC	When Span Type is E1, ITU & CHINA Range: [0, 4065], ANSI Range: [0, 16353]. When Span Type is T1/J1, ITU & CHINA Range: [0, 4072], ANSI Range: [0, 16360].
Assign CIC To D-channel	If set to yes, D-channel will be assigned a CIC. Else, D-channel will not be assigned. By default, it is set to No.
Network Indicator	Network Indicator (NI) should match in nodes, otherwise it might cause issues. Users can select "National", "National Spare", "International", or "International Spare". Usually "National" or "International" is used.

LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0dB unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Codec	Select alaw or ulaw. If set to default, alaw will be used for E1.
Advanced Settings	
Coding	Select "HDB3" or "AMI".
CRC	Select whether to use CRC4 or not.
Called Nature of Address Indicator	Indicates the type of the called number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
Calling Nature of Address Indicator	Indicates the type of the calling number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
D-chan	Indicates the D channel for control
International Prefix National Prefix Subscriber Prefix Unknown Prefix	Configure the prefix in Called Nature of Address Indicator and Calling Nature of Address Indicator for each type.

Table 50: Digital Hardware Configuration Parameters: E1 - MFC/R2

Basic Settings	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it. • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.
Variant	MFC/R2 multinational adaption. UCM6510 supports MFC/R2 standards by ITU and MFC/R2 standards in different countries or regions including

	Argentina, Brazil, China, Czech Republic, Colombia, Ecuador, Indonesia, Mexico, the Philippines and Venezuela.
Get ANI First	If enabled, the callee side will request the caller to send caller number first and then called number. Note: Options "Get ANI First" and "Skip Category" cannot be enabled at the same time.
Category	Select the category of the caller. UCM6510 supports four categories: National Subscriber, National Priority Subscriber, International Subscriber and International Priority Subscriber.
LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0dB unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Play Local RBT	This configured whether to play the ringback tone from local UCM6510 or not. If enabled, the local UCM6510 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default setting is disabled.
Advanced Settings	
Coding	Select "HDB3" or "AMI".
CRC	Select whether to use CRC4 or not.
MF Back Timeout (ms)	MFC/R2 value in milliseconds for MF timeout. Values smaller than 500ms are not recommended. -1 represents default value.
Metering Pulse Timeout (ms)	MFC/R2 value in milliseconds for the metering pulse timeout. Metering pulse is sent by some telcos for some R2 variants during a call presumably for billing purposes to indicate costs. Should not last more than 500ms, -1 represents default value, and for Argentina the default value is 400ms, for others is 0ms.
Alllow Collect Calls	Brazil has a special calling party category for collect calls (llamadas por cobrar) instead of using the operator (as in Mexico). The R2 spec in Brazil says a special GB tone should be used to reject collect calls. By default, this is disabled, which means collect calls will be blocked.
Double Answer	Some PBXs require a double-answer process to block collect calls. If users have problem blocking collect calls using Group B signals, please try enabling this option.

Accept On Offer	By default it's enabled. In most of cases, this option should be enabled.
Skip Category	If enabled, the callee side will request the caller to send caller category before sending caller number. Note: "Get ANI First" and "Skip Category" cannot be enabled at the same time.
Charge Calls	Whether or not report to the other end "accept call with charge". This setting has no effect with most telecos. The default setting is enabled (recommended).
Custom Options	Click on "Custom Options" button (on the right top of the configuration dialog) and then user can customize desired tone and timer options accordingly.

Table 51: Digital Hardware Configuration Parameters: T1/J1 - PRI_NET/PRI_CPE

Basic Settings	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it. • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1/J1 link is the preferred source of the master clock.
LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0dB unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Codec	Select alaw or ulaw. If set to default, ulaw will be used for T1/J1.
Play Local RBT	This configured whether to play the ringback tone from local UCM6510 or not. If enabled, the local UCM6510 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default setting is disabled.
Advanced Settings	
Switch Type	Select switch type. • EuroISDN: EuroISDN (common in Europe)

	• NI2: National ISDN type 2 (common in the US) • DMS100: Nortel DMS100 • 4ESS: AT&T 4ESS • 5ESS: Lucent 5ESS • NI1: old national ISDN type 1 • Q.SIG
Coding	Select "B8ZS" or "AMI".
PRI Dial Plan	This setting is used to specify the type of the callee number. The service provider will usually verify this. The default setting is "unknown". In some very unusual circumstances, you may need set to "Dynamic" or "Redundant". **Note:** When one type is selected, you might not be able to dial another class of numbers. For example, if "National" is configured, you won't be able to dial local or international numbers.
PRI Local Dial Plan	This setting is used to specify the type of the caller number. The service provider will usually verify this.
D-chan	Indicates the D channel for control.
International Prefix National Prefix Local Prefix Private Prefix Unknown Prefix	Configure the prefix in PRI Local Dial Plan and PRI Dial Plan for each type.
PRI T310	Configure PRI T310 Timer (in seconds). The default value is 10 seconds.
PRI Indication	Select the PRI Indication. • outofband: Use RELEASE, DISCONNECT or other messages with CAUSE to indicate call progress (e.g., cause: unassigned number or user busy). • inband: use in-band tones to play busy or congestion signal to the other side. This is the default setting.
Reset Interval	The interval that restarts idle channels.
PRI Exclusive	This setting is used to set up the ChannelID in SETUP message. If enabled, only the specified B channel can be used. Otherwise, select one of the channels in B channel. If you need override the existing channels selection routine and force all PRI channels to be marked as exclusively selected, please enable it.
Facility Enable	If selected, transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility) will be enabled.

NSF	Some switches (AT&T especially) require network specific facility. Currently the supported values are "none", "sdn", "megacom", "tollfreemegacom", "accunet".

Table 52: Digital Hardware Configuration Parameters: T1/J1 - SS7

Basic Settings	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it. • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.
SS7 Variant	Select ITU, ANSI or CHINA.
Originating Point Code	Originating point code is used to identify the node originating the message, always provided by the operator/ISP. • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
Destination Point Code	Destination point code is the address to send the message to, always be provided by the operator/ISP. • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
First CIC	When Span Type is E1, ITU & CHINA Range: [0, 4065], ANSI Range: [0, 16353]. When Span Type is T1/J1, ITU & CHINA Range: [0,4072], ANSI Range: [0, 16360].
Assign CIC to D-Channel	If set to yes, D-channel will be assigned with a CIC. Else, D-channel will not be assigned with a CIC. By default, it is set to No.
Network Indicator	Network Indicator (NI) should match in nodes, otherwise it might cause issues. Users can select "National", "National Spare", "International", or "International Spare". Usually "National" or "International" is used.
LBO	The line build-out (LBO) is the distance between the operators and the PBX. Please use the default value 0dB unless the distance is long.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid

	range is -24dB to +12dB.
Codec	Select alaw or ulaw. If set to default, ulaw will be used for T1/J1.
Advanced Settings	
Coding	Select "B8ZS" or "AMI".
Called Nature of Address Indicator	Indicates the type of the called number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
Calling Nature of Address Indicator	Indicates the type of the calling number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
D-chan	Indicates the D channel for control.
International Prefix National Prefix Subscriber Prefix Unknown Prefix	Configure the prefix in Called Nature of Address Indicator and Calling Nature of Address Indicator for each type.

Table 53: Digital Hardware Configuration Parameters: T1-E&M Immediate/E&M Wink

Basic Setting	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the PBX system clock will synchronize to it. • Master: The port will never be used as a source of timing. This is appropriate when you know the far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1/J1 link is the preferred source of the master clock.
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Codec	Select alaw or ulaw. The default codec is ulaw for T1.
Advance Settings	
Coding	Select B8ZS or AMI. The default setting is B8ZS for T1.
OutgoingDialDelay	The option is only valid for E&M Wink signaling. The dial delay interval

	after received WINK event in an outgoing call. The default value is 200ms.
rxwink	Configure receive wink timing. The default setting is 300ms.

DIGITAL TRUNK CONFIGURATION

After configuring digital hardware, go to web GUI->**PBX**->**Basic/Call Routes**->**Digital Trunks**.

- Click on "Create New Digital Trunk" to add a new digital trunk.
- Click on to configure detailed parameters for the digital trunk.
- Click on to configure Direct Outward Dialing (DOD) for the digital Trunk.
- Click on to delete the digital trunk.

The digital trunk parameters are listed in the table below.

Table 54: Digital Trunk Configuration Parameters

Trunk Name	Configure trunk name to identify the digital trunk.
Channel Group	Configure the digital channel group used by the trunk.
Hide CallerID	Configure to hide outgoing caller ID. The default setting is "No".
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored. When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist: • The CallerID configured for the extension will be looked up first. • If “Keep Trunk CID” is enabled, the CallerID configured for the trunk will be used. • If the above two are missing, the "Global Outbound CID" defined in web GUI->**PBX**->**Internal Options**->**General** will be used.
CallerID Name	Configure the new name of the caller when the extension has no CallerID Name configured.
Auto Record	Enable automatic recording for the calls using this trunk (for SIP trunk

	only). The default setting is disabled. The recording files are saved in external storage device if plugged in and can be accessed under web GUI->**CDR**->**Recording Files**.
Fax Detection	Enable to detect Fax signal from the trunk during the call and send the received Fax to the default Email address in Fax setting page under web GUI->PBX->Internal Options->Fax/T.38. **Note:** If enabled, Fax Pass-through cannot be used.

DIRECT OUTWARD DIALING (DOD) VIA DIGITAL TRUNKS

Please refer to section ***[DIRECT OUTWARD DIALING (DOD) VIA VOIP TRUNKS]***.

DIGITAL TRUNK TROUBLESHOOTING

After configuring the digital trunk on the UCM6510 as described above, if it doesn't work as expected, users can go to capture signaling trace on the UCM6510 web UI for troubleshooting purpose.

Depending on the signaling selected for the digital trunk, users can go to the following pages to capture trace:

- PRI Signaling Trace: web GUI->**Maintenance**->**Troubleshooting** ->**PRI Signaling Trace**
- SS7 Signaling Trace: web GUI->**Maintenance**->**Troubleshooting** ->**SS7 Signaling Trace**
- MFC/R2 Signaling Trace: web GUI->**Maintenance**->**Troubleshooting** ->**MFC/R2 Signaling Trace**
- E&M Trace: web GUI->**Maintenance**->**Troubleshooting**->**E&M Immediate Record Trace**

Here is the step to capture trace:

1. Click on "Start" to start capturing trace. The output result shows "Capturing..."
2. Once the test is done, click on "Stop" to stop the trace.
3. Click on "Download" to download the trace.

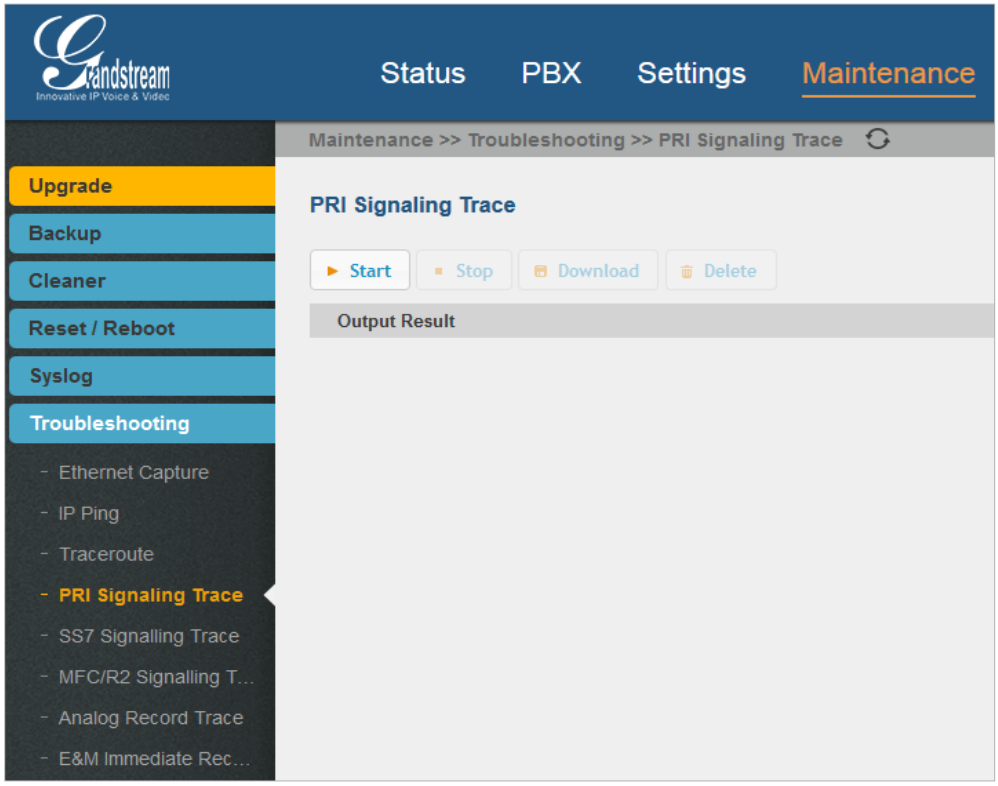


Figure 88: Troubleshooting Digital Trunks

For E&M Immediate Signaling, user could configure “Record Direction” and “Record File Mode”.

After capturing the trace, users can download it for basic analysis. Or you can contact Grandstream Technical support in the following link for further assistance if the issue is not resolved.
http://www.grandstream.com/index.php/support

This page intentionally left blank

DATA TRUNK

The UCM6510 E1/T1/J1 interface also supports data trunk function that allows users to access Internet. Users can select HDLC, HDLC-ETH, Cisco and PPP protocol for the data trunk.

To use data trunk,

1. Go to web UI->**PBX**->**Ports Config**->**Digital Hardware** page and click to create a new group. Designate a channel for data trunk usage in the group setting.
2. Go to web UI->**PBX**->**Basic/Call Routes**->**Data Trunks** page, click on to edit the data trunk.
3. Save the configuration and click on "Apply Changes" for the change to take effect.
4. Once connected, the data trunk will periodically ping and check the status, with status indicator shown for the data trunk on the web page. The status indicator shows if connected successfully.
5. If the user happens to lost connection or experience unstable connection, click on to reconnect to help resolve the problem.
6. Users can always click on ON/OFF switch OFF ON in the web page to enable/disable the configured data trunk.

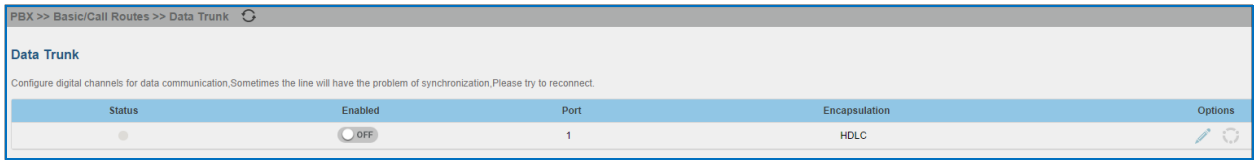


Figure 89: Data Trunk Web Page

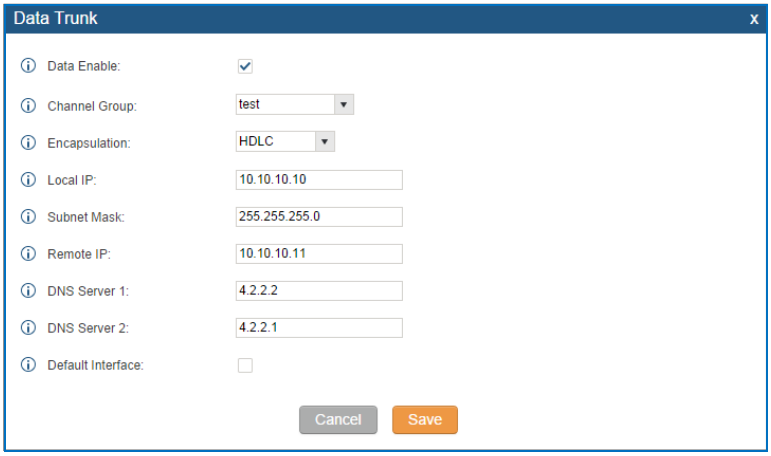


Figure 90: Data Trunk Configuration

Table 55: Data Trunk Configuration Parameters

Data Enable	Select the checkbox to enable/disable data trunk. Users can also click on the ON/OFF switch in data trunk web page to enable/disable this.
Channel Group	Select the digital channel group from the dropdown list to be used for data trunk. Users will need create a new group under web UI->**PBX**->**Ports Config**->**Digital Hardware** page for this purpose.
Encapsulation	Select the protocol used for the data trunk. The UCM6510 supports HDLC, HDLC-ETH, PPP, Cisco and Frame Relay.
Local IP	Configure the local IP address for the data port. This IP address shouldn't conflict with the WAN or LAN side IP of the UCM6510.
Subnet Mask	Configure the subnet mask for the data port.
Remote IP	Configure the remote IP address for the data port. This IP will be the gateway IP address if "Default Interface" is enabled for the datat trunk.
DNS Server 1	Configure DNS server 1.
DNS Server 2	Configure DNS server 2.
Default Interface	If enabled, this data port will be used as the default interface for Internet connection. The "Remote IP" will be the gateway IP address. This has higher priority than the "Default Interface" assignment (LAN 1 or LAN 2) under web UI->**Settings** if "Dual" is selected as the network method.

VOIP TRUNKS

VOIP TRUNK CONFIGURATION

VoIP trunks can be configured in UCM6510 under web GUI->**PBX**->**Basic/Call Routes**->**VoIP Trunks**. Once created, the VoIP trunks will be listed with Provider Name, Type, Hostname/IP, Username and Options to edit/detect the trunk.

- Click on "Create New SIP Trunk" or "Create New IAX Trunk" to add a new VoIP trunk.
- Click on to configure detailed parameters for the VoIP trunk.
- Click on to configure Direct Outward Dialing (DOD) for the SIP Trunk.
- Click on to start LDAP Sync.
- Click on to delete the VoIP trunk.

For VoIP trunk example, please refer to the following document:
http://www.grandstream.com/products/ucm_series/ucm65xx/documents/how_to_interconnect_multiple_ucm6510_using_peer_trunk.pdf

The VoIP trunk options are listed in the table below.

Table 56: Create New SIP Trunk

Type	Select the VoIP trunk type. • Peer SIP Trunk • Register SIP Trunk
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Original CID	Keep the CID from the inbound call when dialing out. This setting will override "Keep Trunk CID" option. Please make sure that the peer PBX at the other side supports to match user entry using "username" field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".

NAT	Turn on this setting when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it is related to NAT configuration or SIP/RTP port support on the firewall.
Disable This Trunk	If checked, the trunk will be disabled. **Note:** If a current SIP trunk is disabled, UCM6510 will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
Need Registration	Select whether the trunk needs to register on the external server or not when "Register SIP Trunk" type is selected. The default setting is No.
Username	Enter the username to register to the trunk from the provider when "Register SIP Trunk" type is selected.
Password	Enter the password to register to the trunk from the provider when "Register SIP Trunk" is selected.
Auth ID	Enter the Authentication ID for "Register SIP Trunk" type.
Auto Record	Enable automatic recording for the calls using this trunk (for SIP trunk only). The default setting is disabled. The recording files can be accessed under web GUI->**CDR**->**Recording Files**.

Table 57: SIP Register Trunk Configuration Parameters

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "All - UDP Primary". • UDP Only • TCP Only • TLS Only • All - UDP Primary: UDP is the primary transport protocol when all the other SIP transport methods are available too. • All - TCP Primary: TCP is the primary transport protocol when all the other SIP transport methods are available too.

	• All – TLS Primary: TLS is the primary transport protocol when all the other SIP transport methods are available too.
Keep Original CID	Keep the CID from the inbound call when dialing out. This setting will override “Keep Trunk CID” option. Please make sure that the peer PBX at the other side supports to match user entry using “username” field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension’s CID when the extension has CID configured. The default setting is “No”.
NAT	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it’s related to NAT configuration or SIP/RTP port configuration on the firewall.
Disable This Trunk	If selected, the trunk will be disabled. **Note:** If a current SIP trunk is disabled, UCM6510 will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
Need Registration	Select whether the trunk needs to register on the external server or not when "Register SIP Trunk" type is selected. The default setting is No.
Username	Enter the username to register to the trunk from the provider when "Register SIP Trunk" type is selected.
Password	Enter the password to register to the trunk from the provider when "Register SIP Trunk" is selected.
Auth ID	Enter the Authentication ID for "Register SIP Trunk" type.
Auto Record	Enable automatic recording for the calls using this trunk (for SIP trunk only). The default setting is disabled. The recording files can be accessed under web GUI->**CDR**->**Recording Files**.
Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263, H.263p.
From Domain	Configure the actual domain name where the extension comes from. This can be used to override the From Header. For example, "trunk.UCM6510.provider.com" is the From Domain in From Header: sip:1234567@trunk.UCM6510.provider.com.

From User	Configure the actual user name of the extension. This can be used to override the From Header. There are cases where there is a single ID for registration (single trunk) with multiple DIDs. For example, "1234567" is the From User in From Header: sip:1234567@trunk.UCM6510.provider.com.
Send PPI Header	If enabled, the SIP INVITE message sent to the trunk will contain PPI (P-Preferred-Identity) header. The default setting is “No”. **Note:** “Send PPI Header” and “Send PAI Header” cannot be enabled at the same time. Only one of the two headers is allowed to be contained in the SIP INVITE message.
Send PAI Header	If enabled, the SIP INVITE message sent to the trunk will contain PAI (P-Asserted-Identity) header. The default setting is “No”. **Note:** “Send PPI Header” and “Send PAI Header” cannot be enabled at the same time. Only one of the two headers is allowed to be contained in the SIP INVITE message.
Outbound Proxy Support	Select to enable outbound proxy in this trunk. The default setting is "No".
Outbound Proxy	When outbound proxy support is enabled, enter the IP address or URL of the outbound proxy.
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	Configure the default DTMF mode when sending DTMF on this trunk. • Default: The global setting of DTMF mode will be used. The global setting for DTMF Mode setting is under web UI->**PBX**->**SIP Settings**->**ToS**. • RFC2833: Send DTMF using RFC2833. • Info: Send DTMF using SIP INFO message. • Inband: Send DTMF using inband audio. This requires 64 bit codec, i.e., PCMU and PCMA. • Auto: Send DTMF using RFC2833 if offered. Otherwise, inband will be used.
Enable Qualify	If enabled, the UCM6510 will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Qualify Timeout	When "Enable Qualify" option is set to "Yes", configure the timeout (in ms) for the Qualify SIP message. If no response is received within the timeout, the device is considered offline. The default setting is 1000ms.

Qualify Frequency	When "Enable Qualify" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limite.
Fax Mode	Select Fax mode. The default setting is “None”. • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->PBX->Internal Options->Fax/T.38.
SRTP	Enable SRTP for the VoIP trunk. The default setting is "No".
CC Settings	
Enable CC	If enabled, the system will automatically alert the user when a called party is available, given that a previous call to that party failed for some reason.
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel is allowed to make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.

Table 58: SIP Peer Trunk Configuration Parameters

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider’s server of the trunk.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "All - UDP Primary". • UDP Only • TCP Only • TLS Only • All - UDP Primary: UDP is the primary transport protocol when all the other SIP transport methods are available too.

	• All - TCP Primary: TCP is the primary transport protocol when all the other SIP transport methods are available too. • All – TLS Primary: TLS is the primary transport protocol when all the other SIP transport methods are available too.
Keep Original CID	Keep the CID from the inbound call when dialing out, this setting will override “Keep Trunk CID” option. Please make sure that the peer PBX at the other side supports to match user entry using “username” field from authentication line.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension’s CID when the extension has CID configured. The default setting is “No”.
NAT	Turn on this option when the PBX is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it’s related to NAT configuration or SIP/RTP port configuration on the firewall.
Disable This Trunk	If selected, the trunk will be disabled. **Note:** If a current SIP trunk is disabled, UCM6510 will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored. When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist: • The CallerID configured for the extension will be looked up first. • If no CallerID configured for the extension, the CallerID configured for the trunk will be used. • If the above two are missing, the "Global Outbound CID" defined in Web GUI->**PBX**->**Internal Options**->**General** will be used.
CallerID Name	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
Auto Record	Enable automatic recording for the calls using this trunk (for SIP trunk only). The default setting is disabled. The recording files can be accessed under web GUI->**CDR**->**Recording Files**.
Advanced Settings	

Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263, H.263p.
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	Configure the default DTMF mode when sending DTMF on this trunk. • Default: The global setting of DTMF mode will be used. The global setting for DTMF Mode setting is under web UI->**PBX**->**SIP Settings**->**ToS**. • RFC2833: Send DTMF using RFC2833. • Info: Send DTMF using SIP INFO message. • Inband: Send DTMF using inband audio. This requires 64 bit codec, i.e., PCMU and PCMA. • Auto: Send DTMF using RFC2833 if offered. Otherwise, inband will be used.
Enable Qualify	If enabled, the UCM6510 will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Qualify Timeout	When "Enable Qualify" option is set to "Yes", configure the timeout (in ms) for the Qualify SIP message. If no response is received within the timeout, the device is considered offline. The default setting is 1000ms.
Qualify Frequency	When "Enable Qualify" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limite.
Fax Mode	Select Fax mode. The default setting is “None”. • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->PBX->Internal Options->Fax/T.38.
SRTP	Enable SRTP for the VoIP trunk. The default setting is "No".
Sync LDAP Enable	If enabled, the local UCM6510 will automatically provide and update the local LDAP contacts to the remote UCM6510 SIP peer trunk. In order to ensure successful synchronization, the remote UCM6510 peer also needs to enable this option on the SIP peer trunk. The default setting is "No".
Sync LDAP Password	This is the password used for LDAP contact file encryption and decryption

	during the LDAP sync process. The password must be the same on both UCM6510 peers to ensure successful synchronization.
Sync LDAP Port	Configure the TCP port used LDAP sync feature between two peer UCM6510.
LDAP Outbound Rule	Specify an outbound rule for LDAP sync feature. The UCM6510 will automatically modify the remote contacts by adding prefix parsed from this rule.
LDAP Dialed Prefix	Specify the prefix for LDAP sync feature. The UCM6510 will automatically modify the remote contacts by adding this prefix.
CC Settings	
Enable CC	If enabled, the system will automatically alert the user when a called party is available, given that a previous call to that party failed for some reason.
CC Max Agents	Configure the maximum number of CCSS agents which may be allocated for this channel. In other words, this number serves as the maximum number of CC requests this channel is allowed to make. The minimum value is 1.
CC Max Monitors	Configure the maximum number of monitor structures which may be created for this device. In other words, this number tells how many callers may request CC services for a specific device at one time. The minimum value is 1.

Table 59: Create New IAX Trunk

Type	Select the VoIP trunk type. • Peer IAX Trunk • Register IAX Trunk
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
Username	Enter the username to register to the trunk from the provider when "Register IAX Trunk" type is selected.
Password	Enter the password to register to the trunk from the provider when "Register IAX Trunk" type is selected.
Disable This Trunk	If selected, the trunk will be disabled.

Table 60: IAX Register Trunk Configuration Parameters

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
Disable This Trunk	If selected, the trunk will be disabled.
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored. When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist: • The CallerID configured for the extension will be looked up first. • If no CallerID configured for the extension, the CallerID configured for the trunk will be used. • If the above two are missing, the "Global Outbound CID" defined in Web GUI->**PBX**->**Internal Options**->**General** will be used.
CallerID Name	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
Username	Enter the username to register to the trunk from the provider.
Password	Enter the password to register to the trunk from the provider.
Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263, H.263p.
Enable Qualify	If enabled, the UCM6510 will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Qualify Timeout	When "Enable Qualify" option is set to "Yes", configure the timeout (in ms) for the Qualify SIP message. If no response is received within the timeout, the device is considered offline. The default setting is 1000ms.
Qualify Frequency	When "Enable Qualify" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limited.

Fax Mode	Select Fax mode. The default setting is “None”. • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->PBX->Internal Options->Fax/T.38.

Table 61: IAX Peer Trunk Configuration Parameters

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider’s server of the trunk.
Keep Trunk CID	If enabled, the trunk CID will not be overridden by extension's CID when the extension has CID configured. The default setting is "No".
Disable This Trunk	If selected, the trunk will be disabled.
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored. When making outgoing calls, the following rules are used to determine which CallerID will be used if they exist: • The CallerID configured for the extension will be looked up first. • If no CallerID configured for the extension, the CallerID configured for the trunk will be used. • If the above two are missing, the "Global Outbound CID" defined in Web GUI->**PBX**->**Internal Options**->**General** will be used.
CallerID Name	Configure the name of the caller to be displayed when the extension has no CallerID Name configured.
Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, ILBC, ADPCM, H.264, H.263, H.263p.
Enable Qualify	If enabled, the UCM6510 will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Qualify Timeout	When "Enable Qualify" option is set to "Yes", configure the timeout (in ms) for the Qualify SIP message. If no response is received within the timeout, the device is considered offline. The default setting is 1000ms.
Qualify Frequency	When "Enable Qualify" option is set to "Yes", configure the interval (in

	seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limited.
Fax Mode	Select Fax mode. The default setting is “None”. • None: Disable Fax. • Fax Detect: Fax signal from the user/trunk during the call can be detected and the received Fax will be sent to the Email address configured for this extension. If no Email address can be found for the user, the Fax will be sent to the default Email address configured in Fax setting page under web UI->PBX->Internal Options->Fax/T.38.

DIRECT OUTWARD DIALING (DOD) VIA VOIP TRUNKS

The UCM6510 provides Direct Outward Dialing (DOD) which is a service of a local phone company (or local exchange carrier) that allows subscribers within a company's PBX system to connect to outside lines directly.

Example of how DOD is used:

Company ABC has a SIP trunk. This SIP trunk has 4 DIDs associated to it. The main number of the office is routed to an auto attendant. The other three numbers are direct lines to specific users of the company. At the moment when a user makes an outbound call their caller ID shows up as the main office number. This poses a problem as the CEO would like their calls to come from their direct line. This can be accomplished by configuring DOD for the CEO’s extension.

Steps on how to configure DOD on the UCM:

1. To setup DOD go to UCM6510 web GUI->**PBX**->**Basic/Call Routes**->**VoIP Trunks** page.
2. Click to access the DOD options for the selected SIP Trunk.
3. Click "Create a new DOD" to begin your DOD setup.
4. For "DOD Number" enter one of the numbers (DIDs) from your SIP trunk provider. In the example above Company ABC received 4 DIDs from their provider. ABC will enter in the number for the CEO's direct line.
5. Select an extension from the "Available Extensions" list. Users have the option of selecting more than one extension. In this case, Company ABC would select the CEO's extension. After making the selection, click on the button to move the extension(s) to the "Selected Extensions" list.

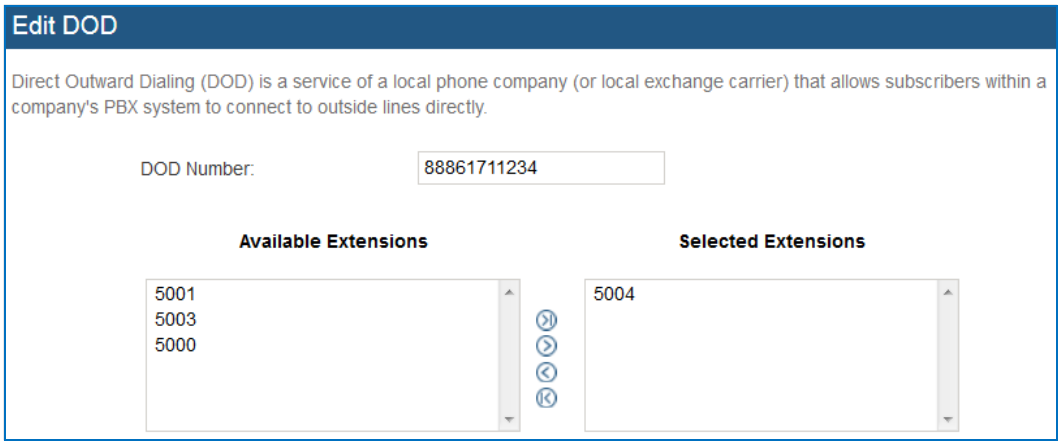

Edit DOD
Direct Outward Dialing (DOD) is a service of a local phone company (or local exchange carrier) that allows subscribers within a company's PBX system to connect to outside lines directly.
DOD Number:
88861711234
Available Extensions
Selected Extensions
5001
5003
5000
5004

Figure 91: DOD extension selection

6. Click "Save" at the bottom.

Once completed, the user will return to the **Edit DOD** page that shows all the extensions that are associated to a particular DOD.

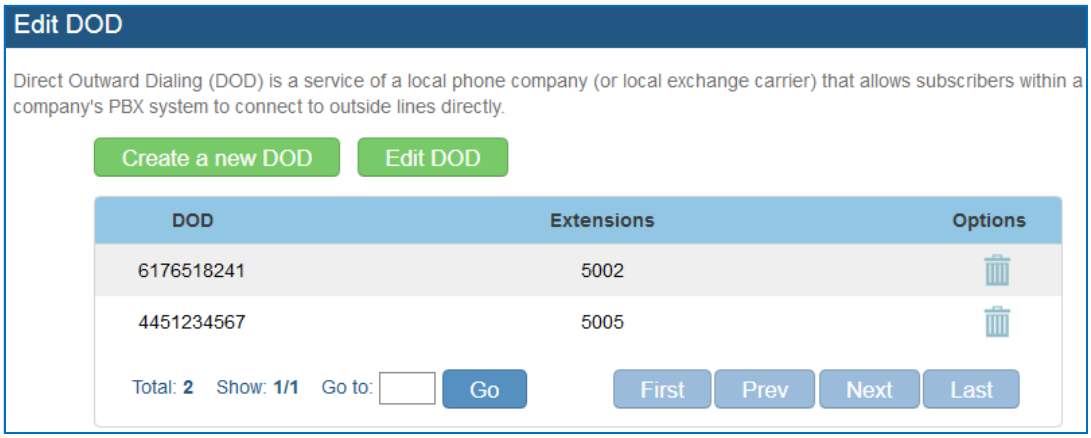


Figure 92: Edit DOD

SLA STATION

UCM6510 supports SLA that allows mapping the key with LED on a multi-line phone to different external lines. When there is an incoming call and the phone starts to ring, the LED on the key will flash in red and the call can be picked up by pressing this key. This allows users to know if the line is occupied or not. The SLA function on the UCM6510 is similar to BLF but SLA is used to monitor external line i.e., analog trunk on the UCM6510. Users could configure the phone with BLF mode on the MPK to monitor the analog trunk status or press the line key pick up call from the analog trunk on the UCM6510.

CREATE/EDIT SLA STATION

SLA Station can be configured on web GUI->**PBX->Basic/Call Routes->SLA Station.**

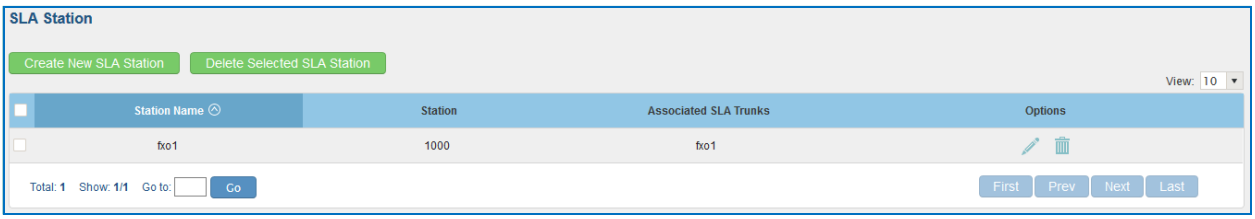


Figure 93: SLA Station

- Click on “Create New SLA Station” to add a SLA Station.
- Click on to edit the SLA Station. The following table shows the SLA Station configuration parameters.
- Click on to delete the SLA Station.

Table 62: SLA Station Configuration Parameters

Station Name	Configure a name to identify the SLA Station.
Station	Specify a SIP extension as a station that will be using SLA.
Available SLA Trunks	Existing Analog Trunks with SLA Mode enabled will be listed here.
Selected SLA Trunks	Select a trunk for this SLA from the Available SLA Trunks list. Click on to arrange the order. If there are multiple trunks selected, when there are calls on those trunks at the same time, pressing the LINE key on the phone will pick up the call on the first trunk here.
SLA Station Options	
Ring Timeout	Configure the time (in seconds) to ring the station before the call is considered unanswered. No timeout is set by default. If set to 0, there will

	be no timeout.
Ring Delay	Configure the time (in seconds) for delay before ringing the station when a call first coming in on the shared line. No delay is set by default. If set to 0, there will be no delay.
Hold Access	This option defines the competence of the hold action for one particular trunk. If set to “open”, any station could hold a call on that trunk or resume one held session; if set to “private”, only the station that places the trunk call on hold could resume the session. The default setting is “open”.

SAMPLE CONFIGURATION

1. On the UCM6510, go to web UI->**Basic/Call Routes**->**Analog Trunks** page. Create analog trunk or edit the existing analog trunk. Make sure “SLA Mode” is enabled for the analog trunk. Once enabled, this analog trunk will be only available for the SLA stations created under web UI->**Basic/Call Routes**->**SLA Station** page.

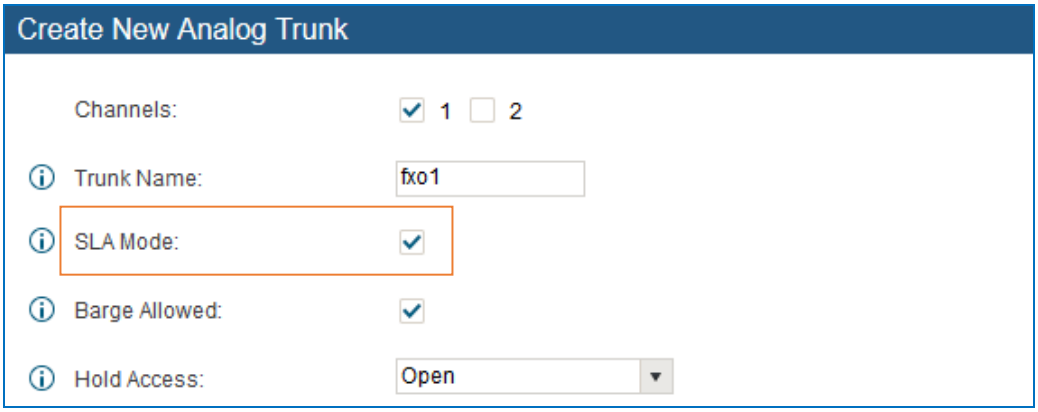


Figure 94: Enable SLA Mode for Analog Trunk

Click on “Save”. The analog trunk will be listed with trunk mode “SLA”.

Figure 95: Analog Trunk with SLA Mode Enabled

2. On the UCM6510, go to web UI->**Basic/Call Routes**->**SLA Station** page, click on “Create New SLA Station”. Please refer to section [CREATE/EDIT SLA STATION] for the configuration parameters. Users can create one or more SLA stations to monitor the analog trunk. The following figure shows two stations, 1002 and 1005, are configured to be associated with SLA trunk “fxo1”.

Station Name	Station	Associated SLA Trunks	Options
sla2	1002	fxo1	
testsla	1005	fxo1	

Figure 96: SLA Example - SLA Station

- On the SIP phone 1, configure to register UCM6510 extension 1002. Configure the MPK as BLF mode and the value must be set to “extension_trunkname”, which is 1002_fxo1 in this case.
- On the SIP phone 2, configure to register UCM6510 extension 1005. Configure the MPK as BLF mode and value must be set to “extension_trunkname”, which is 1005_fxo1 in this case.

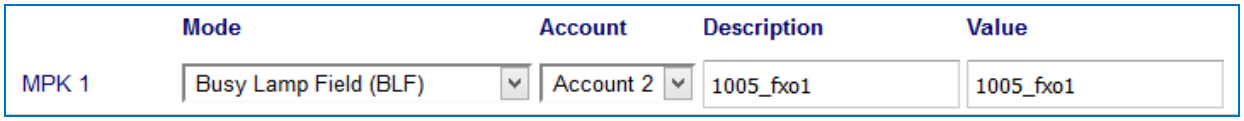


Figure 97: SLA Example - MPK Configuration

Now the SLA station is ready to use. The following functions can be achieved by this configuration.

- Making an outbound call from the station/extension, using LINE key
  When the extension is in idle state, pressing the line key for this extension on the phone to off hook. Then dial the station’s extension number, for example, dial 1002 on phone 1 (or dial 1005 on phone 2), to hear the dial tone. Then the users could dial external number for the outbound call.
- Making an outbound call from the station/extension, using BLF key
  When the extension is in idle state, pressing the MPK and users could dial external numbers directly.
- Answering call using LINE key
  When the station is ringing, pressing the LINE key to answer the incoming call.
- Barging-in active call using BLF key
  When there is an active call between an SLA station and an external number using the SLA trunk, other SLA stations monitoring the same trunk could join the call by pressing the BLF key if “Barge Allowed” is enabled for the analog trunk.
- Hold/Unhold using BLF key
  If the external line is previously put on hold by an SLA station, another station that monitors the same SLA trunk could unhold the call by pressing the BLF key if “Hold Access” is set to “open” on the analog trunk and the SLA station.

This page intentionally left blank

CALL ROUTES

OUTBOUND ROUTES

In the UCM6510, an outgoing calling rule pairs an extension pattern with a trunk used to dial the pattern. This allows different patterns to be dialed through different trunks (e.g., "Local" 7-digit dials through a FXO while "Long distance" 10-digit dials through a low-cost SIP trunk). Users can also set up a failover trunk to be used when the primary trunk fails.

Go to web GUI->**PBX**->**Basic/Call Routes**->**Outbound Routes** to add and edit outbound rules.

- Click on "Create New Outbound Rule" to add a new outbound route.
- Click on to edit the outbound route.
- Click on to delete the outbound route.
- On the UCM6510, the outbound route priority is based on “Best matching pattern”. For example, the UCM6510 has outbound route A with pattern 1xxx and outbound route B with pattern 10xx configured. When dialing 1000 for outbound call, outbound route B will always be used first. This is because pattern 10xx is a better match than pattern 1xxx. Only when there are multiple outbound routes with the same pattern configured, users can click on to move the outbound route up/down to arrange the priority among those outbound routes.

Table 63: Outbound Route Configuration Parameters

Calling Rule Name	Configure the name of the calling rule (e.g., local, long_distance, and etc). Letters, digits, _ and - are allowed.
Pattern	• All patterns are prefixed with the "_". • Special characters: X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. ".": Wildcard. Match one or more characters. "!": Wildcard. Match zero or more characters immediately. Example: [12345-9] - Any digit from 1 to 9.
Password	Configure the password for users to use this rule when making outbound calls.
Call Duration Limit	Once call duration limit is enabled, it will set the maximum duration of call-blocking.

The Maximum call duration	User can customize the maximum call duration (in seconds) that is allowed for the outbound call. By default, this value is set to 0 means there is no limit for the call duration.
Warning Time	This option will give caller warning when call duration is approaching to its limit. If the warning time is set to 'y', the warning tone will be played to caller when y seconds is left to end the call by UCM.
Warning Repeat Interval	Once this option is set to 'z', it will repeatedly warning caller every z seconds after the first warning.
Privilege Level	Select privilege level for the outbound rule. • Internal: The lowest level required. All users can use this rule. • Local: Users with Local, National, or International level are allowed to use this rule. • National: Users with National or International level are allowed to use this rule. • International: The highest level required. Only users with international level can use this rule. The default setting is "Disable". Please be aware of the potential security risks when using "Internal" level, which means all users can use this outbound rule to dial out from the trunk.
Enable Filter on Source Caller ID	When enabled, users could specify extensions allowed to use this outbound route. "Privilege Level" is automatically disabled if using "Enable Filter on Source Caller ID". The following two methods can be used at the same time to define the extensions as the source caller ID. 3. Select available extensions/extension groups from the left to the right. This allows users to specify arbitrary single extensions available in the PBX. 4. Custom Dynamic Route: define the pattern for the source caller ID. This allows users to define extension range instead of selecting them one by one. • All patterns are prefixed with the "_". • Special characters: X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. ".": Wildcard. Match one or more characters. "!": Wildcard. Match zero or more characters immediately. Example: [12345-9] - Any digit from 1 to 9.
Send This Call Through Trunk	

Use Trunk	Select the trunk for this outbound rule.
Strip	Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk. Example: The users will dial 9 as the first digit of a long distance calls. However, 9 should not be sent out via analog lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Use Failover Trunk	
Failover Trunk	Failover trunks can be used to make sure that a call goes through an alternate route, when the primary trunk is busy or down. If "Use Failover Trunk" is enabled and "Failover trunk" is defined, the calls that cannot be placed via the regular trunk may have a secondary trunk to go through. Example: The user's primary trunk is a VoIP trunk and the user would like to use the PSTN when the VoIP trunk is not available. The PSTN trunk can be configured as the failover trunk of the VoIP trunk.
Strip	Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk. Example: The users will dial 9 as the first digit of a long distance calls. However, 9 should not be sent out via analog lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.

INBOUND ROUTES

Inbound routes can be configured via web GUI->**PBX**->**Basic/Call Routes**->**Inbound Routes**.

- Click on "Create New Inbound Rule" button to add a new inbound route.
- Click on "Blacklist" button to configure blacklist for all inbound routes.

- Click on to edit the inbound route.
- Click on to delete the inbound route.

INBOUND RULE CONFIGURATIONS

Table 64: Inbound Rule Configuration Parameters

Trunks	Select the trunk to configure the inbound rule.
DID Pattern	• All patterns are prefixed with the "_". • Special characters: X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. ".": Wildcard. Match one or more characters. "!": Wildcard. Match zero or more characters immediately. Example: [12345-9] - Any digit from 1 to 9. • The pattern can be composed of two parts, divided by a '/' character. The first part is used to specify the dialed number the second part is used to specify the caller ID and it is optional, if set it means only the extension with the specific caller ID is allowed to call in or call out. For example, patter '_2XXX/1234' means the only extension with the caller ID '1234' is allowed to use this rule.
Privilege Level	Select privilege level for the inbound rule when a VoIP trunk is selected in "Trunks" field. • Internal: The lowest level required. All users can use this rule. • Local: Users with Local, National or International level are allowed to use this rule. • National: Users with National or International level are allowed to use this rule. • International: The highest level required. Only users with international level can use this rule. This setting is used to compare with the outbound trunk's permission level when the inbound call dials out via a trunk on the UCM6510. Therefore, it's usually used only when the "Default Destination" is set to "By DID".
Default Destination	Select the default destination for the inbound call. • Extension • Voicemail

	• Conference Room • Call Queue • Ring Group • Paging/Intercom • Voicemail Group • Fax • DISA • IVR • By DID When "By DID" is used, the UCM6510 will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, voicemail groups and Fax extension as configured in "DID destination". If the dialed number matches the DID pattern, the call will be allowed to go through. • Dial By Name
Strip	Specify the number of digits to strip from the beginning of the DID. This is used when "By DID" is selected in "Default Destination".
Prepend	Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.
Prepend Trunk Name	If enabled, the trunk name will be added to the caller id name as the displayed caller id name.
Dial Trunk	Configure to allow the inbound call to dial out from the PBX's trunk or not. The default setting is disabled. Please be aware of potential security risk if "Dial Trunk" is enabled. The inbound call might be able to dial out international calls from the PBX's trunk if allowed by the privilege level.
DID Destination	Select the DID destination if "By DID" is selected in "Default Destination". Only the selected category can be reached by DID using this inbound route. • Extension • Conference • Call Queue • Ring Group • Paging/Intercom Group • IVR • Voicemail Groups • Fax Extension • Dial By Name
Alert-Info	When present in an INVITE request, the Alert-Info header field specifies an alternative ring tone to the UAS.

Time Condition	
Start Time	Select the start time "hour:minute" for the trunk to use the inbound rule.
End Time	Select the end time "hour:minute" for the trunk to use the inbound rule.
Date	Select "By Week" or "By Day" and specify the date for the trunk to use the inbound rule.
Week	Select the day in the week to use the inbound rule.
Destination	Select the destination for the inbound call under the defined time condition. • Extension • Voicemail • Conference Room • Call Queue • Ring Group • Paging/Intercom • Voicemail Group • Fax • DISA • IVR • By DID When "By DID" is used, the UCM6510 will look for the destination based on the number dialed, which could be local extensions, conference, call queue, ring group, paging/intercom group, IVR, voicemail groups and Fax extension as configured in "DID destination". If the dialed number matches the DID pattern, the call will be allowed to go through. Configure the number of digits to be stripped in "Strip" option. • Dial By Name

INBOUND ROUTE: PREPEND EXAMPLE

UCM6510 now allows user to prepend digits to an inbound DID pattern, with strip taking precedence over prepend. With the ability to prepend digits in inbound route DID pattern, user no longer needs to create multiple routes for the same trunk in order to route calls to different extensions.

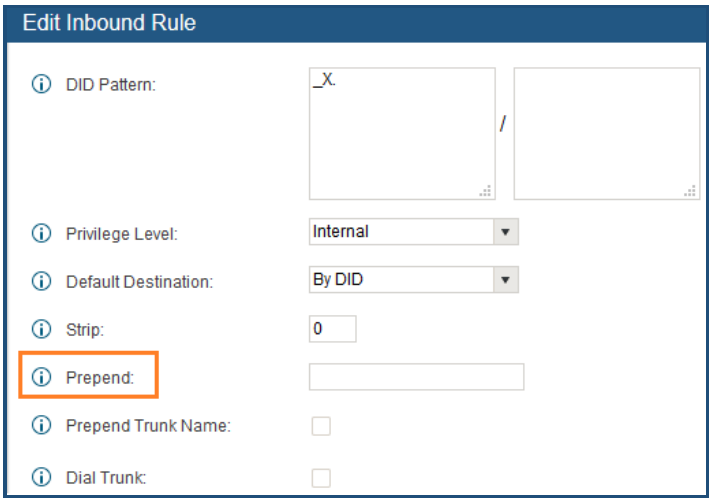


Figure 98: Inbound Route feature: Prepend

The following example demonstrates the process,

1. If Trunk provides a DID pattern of 18005251163.
2. If **Strip** is set to 8, UCM6510 will strip the first 8 digits.
3. If **Prepend** is set to 2, UCM6510 will then prepend a 2 to the stripped number, now the number become 2163.
4. UCM6510 will now forward the incoming call to extension 2163.

BLACKLIST CONFIGURATIONS

In the UCM6510, Blacklist is supported for all inbound routes. Users could enable the Blacklist feature, manage the Blacklist by clicking on "Blacklist".

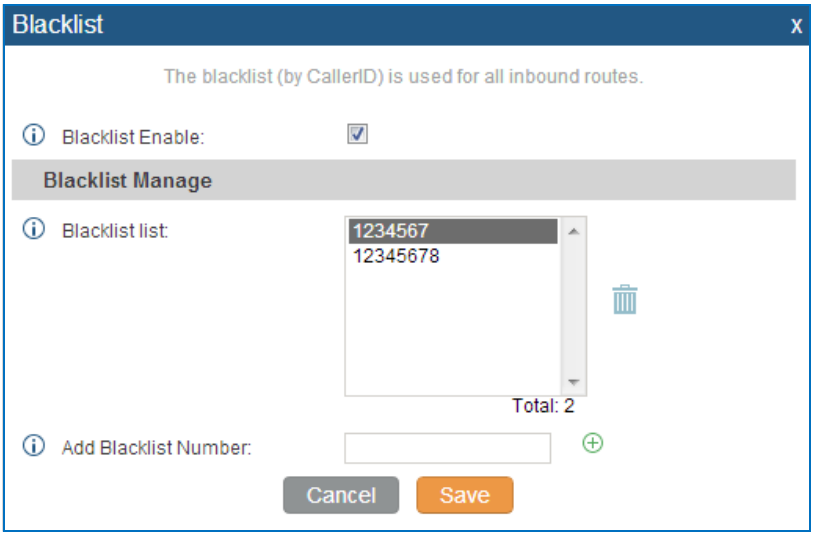


Figure 99: Blacklist Configuration Parameters

- Select the checkbox for "Blacklist Enable" to turn on Blacklist feature for all inbound routes. Blacklist is disabled by default.
- Enter a number in "Add Blacklist Number" field and then click to add to the list.
- To remove a number from the Blacklist, select the number in "Blacklist list" and click on .

Note:

Users could also add a number to the Blacklist or remove a number from the Blacklist by dialing the feature code for "Blacklist Add' (default: *40) and "Blacklist Remove" (default: *41) from an extension. The feature code can be configured under web GUI->**PBX**->**Internal Options**->**Feature Codes**.

CONFERENCE BRIDGE

The UCM6510 supports Conference Bridge allowing 64 participants with up to 8 bridges at the same time. The conference bridge configurations can be accessed under web GUI->**PBX**->**Call Features**->**Conference**. In this page, users could create, edit, view, invite, manage the participants and delete conference bridges. The conference bridge status and conference call recordings (if recording is enabled) will be displayed in this web page as well.

CONFERENCE BRIDGE CONFIGURATIONS

- Click on "Create New Conference Room" to add a new conference bridge.
- Click on to edit the conference bridge.
- Click on to delete the conference bridge.

Table 65: Conference Bridge Configuration Parameters

Extension	Configure the conference number for the users to dial into the conference.
Password	When configured, the users who would like to join the conference call must enter this password before accessing the conference bridge. **Note:** • If "Public Mode" is enabled, the password is not required to join the conference bridge thus this field is invalid. • The password has to be at least 4 characters.
Admin Password	Configure the password to join the conference bridge as administrator. Conference administrator can manage the conference call via IVR (if "Enable Caller Menu" is enabled) as well as invite other parties to join the conference by dialing "0" (permission required from the invited party) or "1" (permission not required from the invited party) during the conference call. **Note:** • If "Public Mode" is enabled, the password is not required to join the conference bridge thus this field is invalid. • The password has to be at least 4 characters.
Enable Caller Menu	If enabled, conference participant could press the * key to access the conference bridge menu. The default setting is "No".
Record Conference	If enabled, the calls in this conference bridge will be recorded automatically

	in a .wav format file. All the recording files will be displayed and can be downloaded in the conference web page. The default setting is "No".
Quiet Mode	If enabled, if there are users joining or leaving the conference, voice prompt or notification tone won't be played. The default setting is "No". **Note:** "Quiet Mode" and "Announce Callers" cannot be enabled at the same time.
Wait For Admin	If enabled, the participants will not hear each other until the conference administrator joins the conference. The default setting is "No". **Note:** If "Quiet Mode" is enabled, the voice prompt for "Wait For Admin" will not be announced.
Enable User Invite	If enabled, users could press 0 to invite other users (with the users' permission) or press 1 to invite other users (without the user's permission) to join the conference. The default setting is "No". **Note:** Conference administrator can always invite other users without enabling this option.
Announce Callers	If enabled, the caller will be announced to all conference participants when there the caller joins the conference. The default setting is "No". **Note:** "Quiet Mode" and "Announce Callers" cannot be enabled at the same time.
Public Mode	If enabled, no authentication will be required when joining the conference call. The default setting is "Yes".
Play Hold Music For First Caller	If enabled, the UCM6510 will play Hold music to the first participant in the conference until another user joins in. The default setting is "No".
Music On Hold	Select the music on hold class to be played in conference call. This option shows up if "Play Hold Music For First Caller" is enabled. Music On Hold class can be set up under web UI->**PBX**->**Internal Options**->**Music On Hold**.
Skip Authentication When Inviting User via Trunk from web GUI	If enabled, the invitation from web GUI for a conference bridge with password will skip the authentication for the invited users. The default setting is "No".

JOIN A CONFERENCE CALL

Users could dial the conference bridge extension to join the conference. If password is required, enter the password to join the conference as a normal user, or enter the admin password to join the conference as administrator.

INVITE OTHER PARTIES TO JOIN CONFERENCE

When using the UCM6510 conference bridge, there are two ways to invite other parties to join the conference.

- **Invite from web GUI**

For each conference bridge in UCM6510 web GUI->**PBX**->**Call Features**->**Conference**, there is an icon for option "Invite a participant". Click on it and enter the number of the party you would like to invite. Then click on "Add". A call will be sent to this number to join it into the conference.

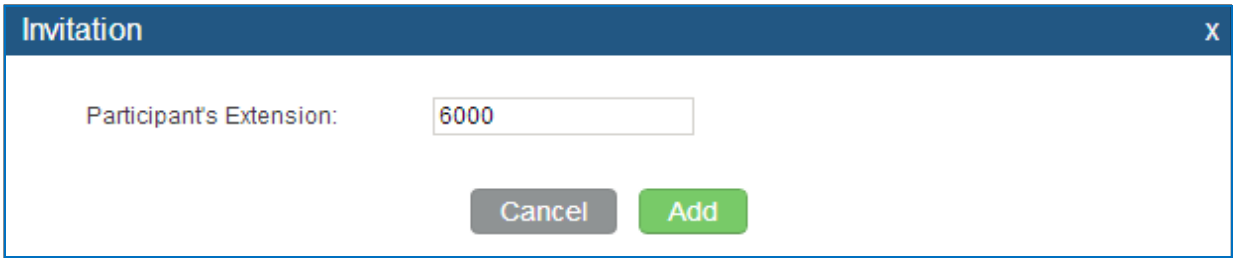


Figure 100: Conference Invitation From web GUI

- **Invite by dialing 0 or 1 during conference call**

  A conference participant can invite other parties to the conference by dialing from the phone during the conference call. Please make sure option "Enable User Invite" is turned on for the conference bridge first. Enter 0 or 1 during the conference call. Follow the voice prompt to input the number of the party you would like to invite. A call will be sent to this number to join it into the conference.

  0: If 0 is entered to invite other party, once the invited party picks up the invitation call, a permission will be asked to "accept" or "reject" the invitation before joining the conference.
  1: If 1 is entered to invite other party, no permission will be required from the invited party.

Note:

Conference administrator can always invite other parties from the phone during the call by entering 0 or 1. To join a conference bridge as administrator, enter the admin password when joining the conference. A conference bridge can have multiple administrators.

DURING THE CONFERENCE

During the conference call, users can manage the conference from web GUI or IVR.

- Manage the conference call from web GUI.

  Log in UCM6510 web GUI during the conference call, the participants in each conference bridge will be listed.

  1. Click on to kick a participant from the conference.
  2. Click on to mute the participant.
  3. Click on to lock this conference bridge so that other users cannot join it anymore.
  4. Click on to invite other users into the conference bridge.

- Manage the conference call from IVR.

  If "Enable Caller Menu" is enabled, conference participant can input * to enter the IVR menu for the conference. Please see options listed in the table below.

Table 66: Conference Caller IVR Menu

Conference Administrator IVR Menu	
1	Mute/unmute yourself.
2	Lock/unlock the conference bridge.
3	Kick the last joined user from the conference.
4	Decrease the volume of the conference call.
6	Increase the volume of the conference call.
7	Decrease your volume.
9	Increase your volume.
8	More options: • 1: List all users currently in the conference call. • 2: Kick all non-Administrator participants from the conference call. • 3: Mute/Unmute all non-Administrator participants from the conference call. • 4: Enable/disable conference call recording. • 8: Exit the caller menu and return to the conference.
Conference User IVR Menu	
1	Mute/unmute yourself.

4	Decrease the volume of the conference call.
6	Increase the volume of the conference call.
7	Decrease your volume.
9	Increase your volume.
8	Exit the caller menu and return to the conference.

Note:

When there is participant in the conference, the conference bridge configuration cannot be modified.

RECORD CONFERENCE

The UCM6510 allows users to record the conference call and retrieve the recording from web GUI->**PBX**->**Call Features**->**Conference**.

To record the conference call, when the conference bridge is in idle, enable "Record Conference" from the conference bridge configuration dialog. Save the setting and apply the change. When the conference call starts, the call will be automatically recorded in .wav format.

The recording files will be listed as below once available. Users could click on to download the recording or click on to delete the recording.

Name	Room	Date	Size	Options
meetme-conf-rec-6300-1372865271.25.wav	6300	2013-07-03 12:39:38 UTC-03:00	10.61 MB	
meetme-conf-rec-6300-1372451238.6.wav	6300	2013-06-28 17:27:46 UTC-03:00	120.04 KB	
meetme-conf-rec-6300-1372205127.347.wav	6300	2013-06-25 21:05:56 UTC-03:00	82.86 KB	
meetme-conf-rec-6300-1372867161.40.wav	6300	2013-07-03 13:10:29 UTC-03:00	10.17 MB	
meetme-conf-rec-6300-1372864546.12.wav	6300	2013-07-03 12:16:01 UTC-03:00	35.67 KB	
meetme-conf-rec-6300-1372866438.36.wav	6300	2013-07-03 12:47:47 UTC-03:00	322.86 KB	
meetme-conf-rec-6300-1372204987.337.wav	6300	2013-06-25 21:03:30 UTC-03:00	315.98 KB	
meetme-conf-rec-6300-1372864583.17.wav	6300	2013-07-03 12:16:36 UTC-03:00	65.67 KB	
meetme-conf-rec-6300-1370385024.71.wav	6300	2013-06-04 19:35:28 UTC-03:00	4.22 MB	

Figure 101: Conference Recording

This page intentionally left blank

IVR

CONFIGURE IVR

IVR configurations can be accessed under the UCM6510 web GUI->**PBX**->**Call Features**->**IVR**. Users could create, edit, view and delete an IVR.

- Click on "Create New IVR" to add a new IVR.
- Click on to edit the IVR configuration.
- Click on to delete the IVR.

Table 67: IVR Configuration Parameters

Basic Settings	
Name	Configure the name of the IVR. Letters, digits, _ and - are allowed.
Extension	Enter the extension number for users to access the IVR.
Dial Other Extensions	If enabled, all callers to the IVR can dial other extensions. The default setting is "No".
Dial Trunk	If enabled, all callers to the IVR is allowed to use trunk. The permission must be configured for the users to use the trunk first. The default setting is "No".
Permission	Assign permission level for outbound calls if "Dial Trunk" is enabled. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". If the user tries to dial outbound calls after dialing into the IVR, the UCM6510 will compared the IVR's permission level with the outbound route's privilege level. If the IVR's permission level is higher than (or equal to) the outbound route's privilege level, the call will be allowed to go through.
Welcome Prompt	Select an audio file to play as the welcome prompt for the IVR. Click on "Prompt" to add additional audio file under web GUI->**Internal Options**->**IVR Prompt**.
Digit Timeout	Configure the timeout between digit entries. After the user enters a digit, the user needs to enter the next digit within the timeout. If no digit is detected within the timeout, the UCM6510 will consider the entries complete. The default timeout is 3 seconds.
Response Timeout	After playing the prompts in the IVR, the UCM6510 will wait for the DTMF entry within the timeout (in seconds). If no DTMF entry is detected within

	the timeout, a timeout prompt will be played. The default setting is 10 seconds.
Response Timeout Prompt	Select the prompt message to be played when timeout occurs.
Invalid Prompt	Select the prompt message to be played when an invalid extension is pressed.
Response Timeout Repeat Loops	Configure the number of times to repeat the prompt if no DTMF input is detected. When the loop ends, it will go to the timeout destination if configured, or hang up. The default setting is 3.
Invalid Repeat Loops	Configure the number of times to repeat the prompt if the DTMF input is invalid. When the loop ends, it will go to the invalid destination if configured, or hang up. The default setting is 3.
Language	Select the voice prompt language to be used for this IVR. The default setting is "Default" which is the selected voice prompt language under web GUI->**PBX**->**Internal Options**->**Language**. The dropdown list shows all the current available voice prompt languages on the UCM6510. To add more languages in the list, please download voice prompt package by selecting "Check Prompt List" under web GUI->**PBX**->**Internal Options**->**Language**.
Key Pressing Events	
Key Press Event: Press 0 Press 1 Press 2 Press 3 Press 4 Press 5 Press 6 Press 7 Press 8 Press 9 Press * Timeout Invalid	Select the event for each key pressing for 0-9, *, Timeout and Invalid. The event options are: 7. Extension 8. Voicemail 9. Conference Rooms 10. Voicemail Group 11. IVR 12. Ring Group 13. Queues 14. Page Group 15. Fax 16. Custom Prompt 17. Hangup 18. DISA 19. Dial By Name 20. External Number 21. Callback

CREATE IVR PROMPT

To record new IVR prompt or upload IVR prompt to be used in IVR, click on "Prompt" next to the "Welcome Prompt" option and the users will be redirected to IVR Prompt page. Or users could go to web GUI->**PBX**->**Internal Options**->**Custom Prompt** page directly.

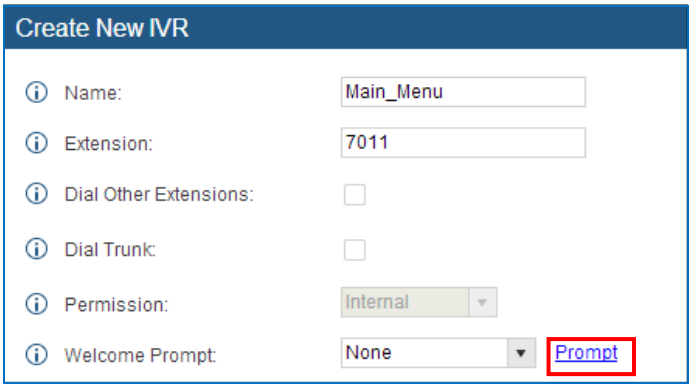


Figure 102: Click On Prompt To Create IVR Prompt

Once the IVR prompt file is successfully added to the UCM6510, it will be added into the prompt list options for users to select in different IVR scenarios.

RECORD NEW IVR PROMPT

In the UCM6510 web GUI->**PBX**->**Internal Options**->**Custom Prompt** page, click on "Record New IVR Prompt" and follow the steps below to record new IVR prompt.

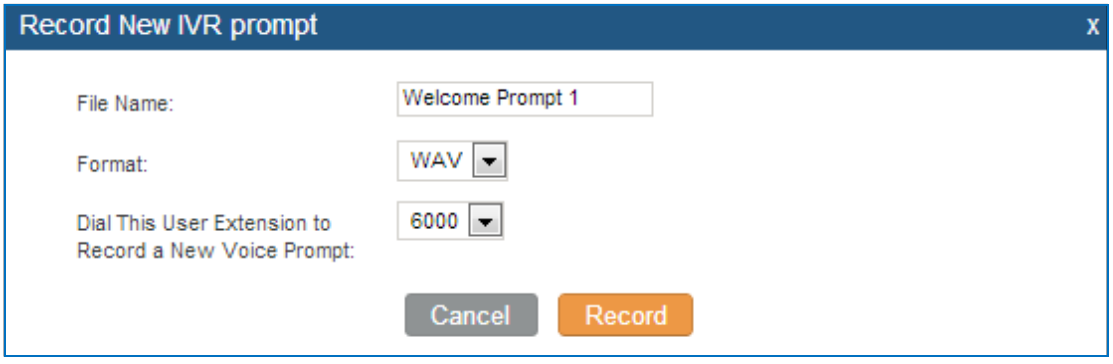


Figure 103: Record New IVR Prompt

- Specify the IVR file name.
- Select the format (GSM or WAV) for the IVR prompt file to be recorded.
- Select the extension to receive the call from the UCM6510 to record the IVR prompt.
- Click the "Record" button. A request will be sent to the UCM6510. The UCM6510 will then call the extension for recording the IVR prompt from the phone.

- Pick up the call from the extension and start the recording following the voice prompt.
- The recorded file will be listed in the IVR Prompt web page. Users could select to re-record, play or delete the recording.

UPLOAD IVR PROMPT

If the user has a pre-recorded IVR prompt file, click on "Upload IVR Prompt" in web GUI->**PBX**->**Internal Options**->**IVR Prompt** page to upload the file to the UCM6510. The following are required for the IVR prompt file to be successfully uploaded and used by the UCM6510:

- PCM encoded.
- 16 bits.
- 8000Hz mono.
- In .mp3 or .wav format; or raw/ulaw/alaw/gsm file with .ulaw or .alaw suffix.
- File size under 5M.

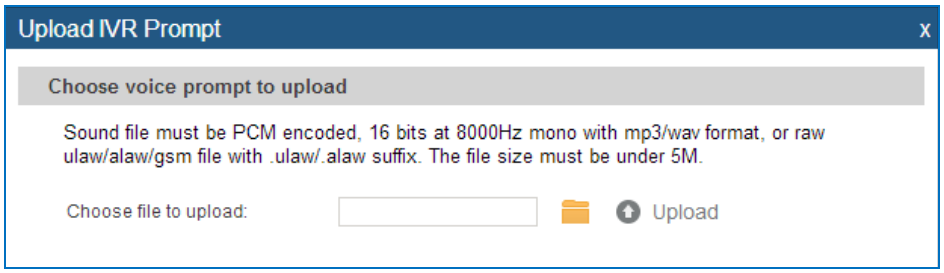

Upload IVR Prompt
x
Choose voice prompt to upload
Sound file must be PCM encoded, 16 bits at 8000Hz mono with mp3/wav format, or raw ulaw/alaw/gsm file with .ulaw/.alaw suffix. The file size must be under 5M.
Choose file to upload:
Upload

Figure 104: Upload IVR Prompt

Click on to select audio file from local PC and click on to start uploading. Once uploaded, the file will appear in the IVR Prompt web page.

LANGUAGE SETTINGS FOR VOICE PROMPT

The UCM6510 supports multiple languages in web GUI as well as system voice prompt. The following languages are currently supported in system voice prompt:

English (United States)
Arabic
Chinese
Dutch
English (United Kingdom)
French
German
Greek
Hebrew
Italian
Polish
Portuguese
Russian
Spanish
Swedish
Turkish

English (United States) and Chinese voice prompts are built in with the UCM6510 already. The other languages provided by Grandstream can be downloaded and installed from the UCM6510 web GUI directly. Additionally, users could customize their own voice prompts, package them and upload to the UCM6510.

Language settings for voice prompt can be accessed under web GUI->**PBX**->**Internal Options**->**Language**.

DOWNLOAD AND INSTALL VOICE PROMPT PACKAGE

To download and install voice prompt package in different languages from UCM6510 web GUI, click on "Check Prompt List" button.

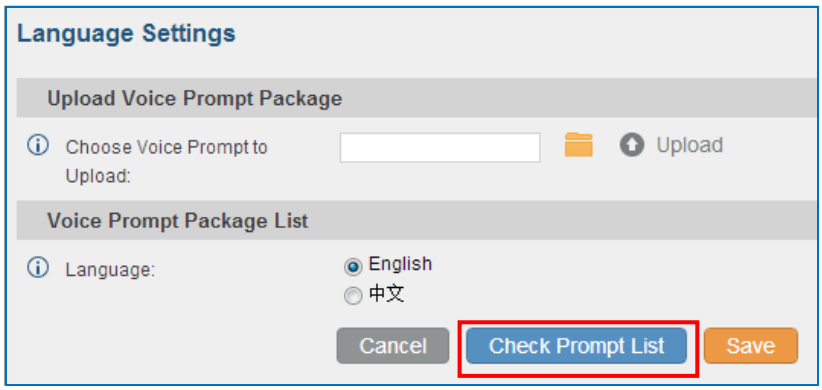


Figure 105: Language Settings for Voice Prompt

A new dialog window of voice prompt package list will be displayed. Users can see the version number (latest version available V.S. current installed version), package size and options to upgrade or download the language.

Figure 106: Voice Prompt Package List

Click on to download the language to the UCM6510. The installation will be automatically started once the downloading is finished.

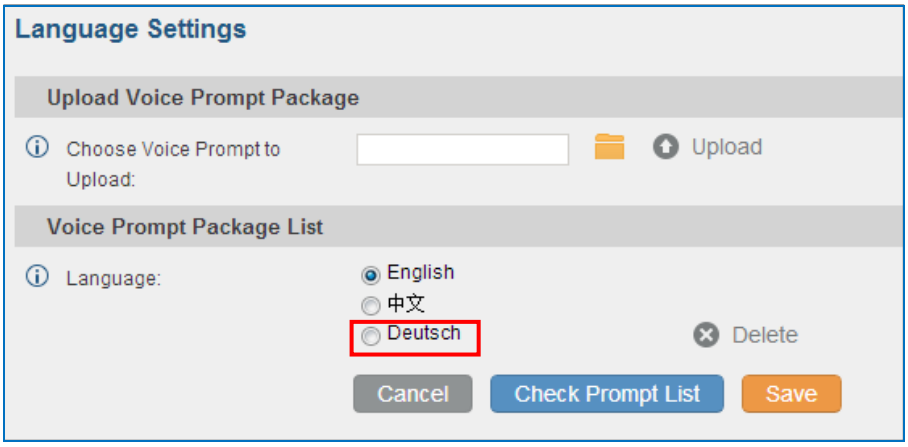


Figure 107: New Voice Prompt Language Added

A new language option will be displayed after successfully installed. Users then could select it to apply in the UCM6510 system voice prompt or delete it from the UCM6510.

This page intentionally left blank

VOICEMAIL

CONFIGURE VOICEMAIL

If the voicemail is enabled for UCM6510 extensions, the configurations of the voicemail can be globally set up and managed under web GUI->**PBX**->**Call Features**->**Voicemail**.

Table 68: Voicemail Settings

Max Greeting	Configure the maximum number of seconds for the voicemail greeting. The default setting is 60 seconds.
Dial '0' For Operator	If enabled, the caller can press 0 to exit the voicemail application and connect to the configured operator's extension. The operator extension can be configured under web GUI->**PBX**->**Internal Options**->**General**.
Max Messages Per Folder	Configure the maximum number of messages per folder in users' voicemail. The valid range 10 to 1000. The default setting is 50.
Max Message Time	Select the maximum duration of the voicemail message. The message will not be recorded if the duration exceeds the max message time. The default setting is 15 minutes. The available options are: • 1 minute • 2 minutes • 5 minutes • 15 minutes • 30 minutes • Unlimited
Min Effective Message Time	Configure the minimum effective duration (in seconds) of a voicemail message. Messages will be automatically deleted if the duration is shorter than the Min Effective Message Time. The default setting is 3 seconds. The available options are: • No minimum • 1 second • 2 seconds • 3 seconds • 4 seconds • 5 seconds **Note:** Silence and noise duration are not counted in message time.
Announce Message Caller-ID	If enabled, the caller ID of the user who has left the message will be

	announced at the beginning of the voicemail message. The default setting is "No".
Announce Message Duration	If enabled, the message duration will be announced at the beginning of the voicemail message. The default setting is "No".
Play Envelope	If enabled, a brief introduction (received time, received from, and etc) of each message will be played when accessed from the voicemail application. The default setting is "Yes".
Play from Last	If enabled, UCM6510 will play from the voice message left most recently; if disabled, UCM6510 will play from the earliest left voice message
Allow User Review	If enabled, users can review the message following the IVR before sending the message out. The default setting is "No".

ACCESS VOICEMAIL

If the voicemail is enabled for UCM6510 extensions, the users can dial the voicemail access feature code (by default *98 or *97) to access the extension's voicemail. The users will be prompt to enter the voicemail password and then can enter digits from the phone keypad to navigate in the IVR menu for different options.

Table 69: Voicemail IVR Menu

Main Menu	Sub Menu 1	Sub Menu 2
1 - New messages	3 - Advanced options	1 - Send a reply
		2 - Call the person who sent this message
		3 - Hear the message envelop
		4 - Leave a message
		* - Return to the main menu
	5 - Repeat the current message	
	7 - Delete this message	
	8 - Forward the message to another user	
	9 – Save	
	* - Help	
	# - Exit	
2 - Change folders	0 - New messages	
	1 - Old messages	
	2 - Work messages	
	3 - Family messages	
	4 - Friend messages	

	# - Cancel	
3 - Advanced options	1 - Send a reply	
	2 - Call the person who sent this message	
	3 - Hear the message envelop	
	4 - Leave a message	
	* - Return to the main menu	
0 - Mailbox options	1 - Record your unavailable message	1 - Accept this recording
		2 - Listen to it
		3 - Re-record your message
	2 - Record your busy message	1 - Accept this recording
		2 - Listen to it
		3 - Re-record your message
	3 - Record your name	1 - Accept this recording
		2 - Listen to it
		3 - Re-record your message
	4 - Record temporary greeting	1 - Accept this recording
		2 - Listen to it
		3 - Re-record your message
	5 - Change your password	
	* - Return to the main menu	

VOICEMAIL EMAIL SETTINGS

The UCM6510 can be configured to send the voicemail as attachment to Email. Click on "Voicemail Email Settings" button to configure the Email attributes and content.

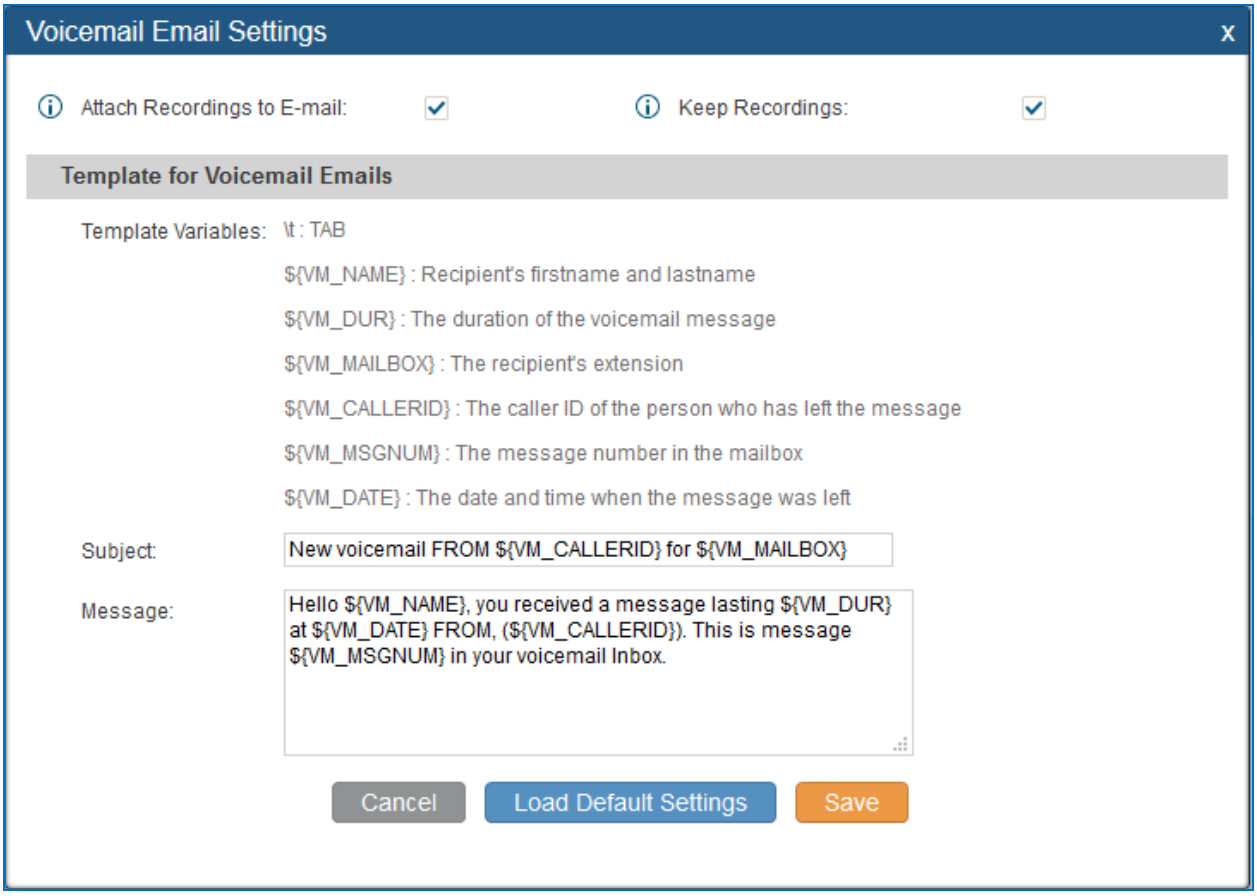

Voicemail Email Settings
x
Attach Recordings to E-mail:
Keep Recordings:
Template for Voicemail Emails
Template Variables:
\t : TAB
${VM_NAME} : Recipient's firstname and lastname
${VM_DUR} : The duration of the voicemail message
${VM_MAILBOX} : The recipient's extension
${VM_CALLERID} : The caller ID of the person who has left the message
${VM_MSGNUM} : The message number in the mailbox
${VM_DATE} : The date and time when the message was left
Subject:
New voicemail FROM ${VM_CALLERID} for ${VM_MAILBOX}
Message:
Hello ${VM_NAME}, you received a message lasting ${VM_DUR} at ${VM_DATE} FROM, (${VM_CALLERID}). This is message ${VM_MSGNUM} in your voicemail Inbox.
Cancel
Load Default Settings
Save

Figure 108: Voicemail Email Settings

Click on "Load Default Settings" button to view the default template as an example.

Table 70: Voicemail Email Settings

Attach Recordings to E-Mail	If enabled, voicemails will be sent to user's Email address. The default setting is "Yes".
Keep Recordings	If enabled, voicemail will be stored in the UCM6510 after email is sent. The default setting is “Yes”.
Template For Voicemail Emails	Fill in the "Subject:" and "Message:" content, to be used in the Email when sending to the user. The template variables are: • \t: TAB • ${VM_NAME}: Recipient's first name and last name • ${VM_DUR}: The duration of the voicemail message • ${VM_MAILBOX}: The recipient's extension • ${VM_CALLERID}: The caller ID of the person who has left the

	message • ${VM_MSGNUM}: The number of messages in the mailbox • ${VM_DATE}: The date and time when the message is left

CONFIGURE VOICEMAIL GROUP

The UCM6510 supports voicemail group and all the extensions added in the group will receive the voicemail to the group extension. The voicemail group can be configured under web GUI->**PBX**->**Call Features**->**Voicemail Group**. Click on "Create New Voicemail Group" to configure the group.

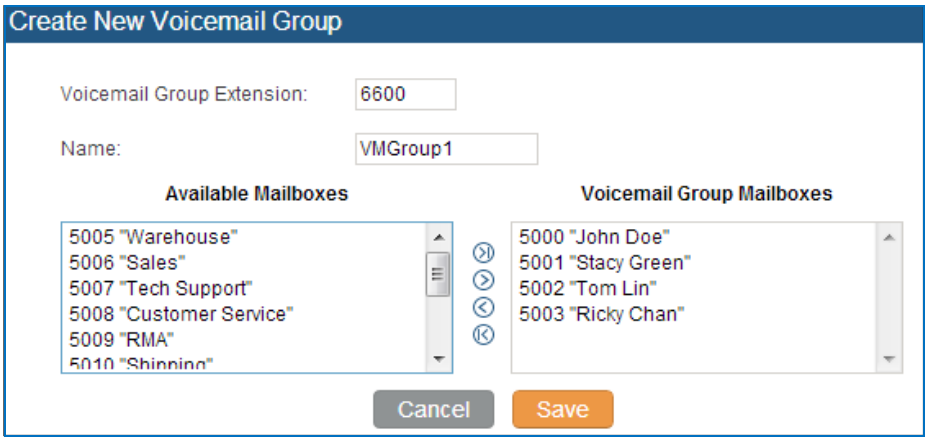


Figure 109: Voicemail Group

Table 71: Voicemail Group Settings

Voicemail Group Extension	Enter the Voicemail Group Extension. The voicemail messages left to this extension will be forwarded to all the voicemail group members.
Name	Configure the Name to identify the voicemail group. Letters, digits, _ and - are allowed.
Voicemail Password	The Voicemail password for the user to check Voicemail messages.
Email Address	The Email address of current user.
Voicemail Group Mailboxes	Select available mailboxes from the left list and add them to the right list. The extensions need to have voicemail enabled to be listed in available mailboxes list.

This page intentionally left blank

RING GROUP

The UCM6510 supports ring group feature with different ring strategies applied to the ring group members. This section describes the ring group configuration on the UCM6510.

CONFIGURE RING GROUP

Ring group settings can be accessed via web GUI->**PBX**->**Call Features**->**Ring Group**.

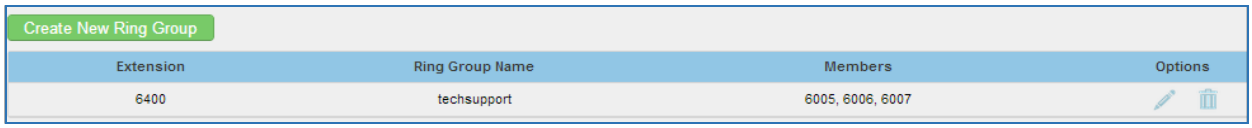


Figure 110: Ring Group

- Click on "Create New Ring Group" to add ring group.
- Click on to edit the ring group. The following table shows the ring group configuration parameters.
- Click on to delete the ring group.

Table 72: Ring Group Parameters

Ring Group Name	Configure ring group name to identify the ring group. Letters, digits, _ and - are allowed.
Extension	Configure the ring group extension.
Ring Group Members	Select available users from the left side to the ring group member list on the right side. Click on to arrange the order.
Ring Strategy	Select the ring strategy. The default setting is "Ring in order". • Ring simultaneously Ring all the members at the same time when there is incoming call to the ring group extension. If any of the member answers the call, it will stop ringing. • Ring in order Ring the members with the order configured in ring group list. If the first member doesn't answer the call, it will stop ringing the first member and start ringing the second member.
Permission	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".

Custom Prompt	This option allows user to customize prompt for a ring group to announce to caller. The file can be uploaded from web GUI->Internal Options->Custom Prompt, or click the 'Prompt' to add additional record.
Ring Timeout on Each Member	Configure the number of seconds to ring each member. If set to 0, it will keep ringing. The default setting is 30 seconds. **Note:** The actual ring timeout might be overridden by users if the phone has ring timeout settings as well.
Auto Record	Once this option is enabled, the calls using this extension or trunk will be automatically recorded.
Enable Destination	If enabled, users could select extension, voicemail, ring group, IVR, call queue, voicemail group as the destination if the call to the ring group has no answer. Secret and Email address are required if voicemail is selected as the destination.
Secret	Configure the password to access the ring group extension's voicemail. **Note:** The password has to be at least 4 characters.
Email Address	Configure the Email address of the ring group extension's voicemail. If "Attach Recordings to E-mail" is enabled from web GUI->**PBX**->**Voicemail**->**Voicemail Email Settings**, the voicemail can be sent to the ring group's Email address as attachment.

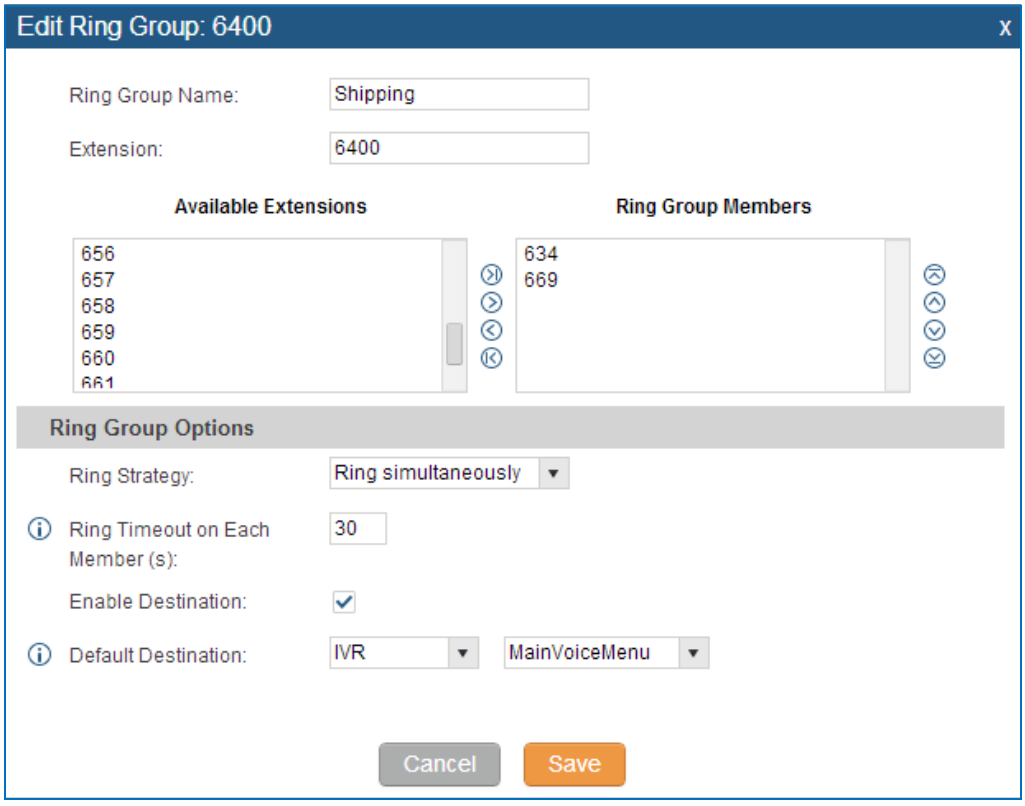
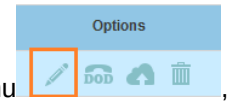


Figure 111: Ring Group Configuration

REMOTE EXTENSION IN RING GROUP

Remote extensions from the peer trunk of a remote UCM6510 can be included in the ring group with local extension. An example of Ring Group with peer extensions is presented in the following:

1. Creating SIP Peer Trunk between both UCM6510_A and UCM6510_B. **SIP Trunk** can be found under web **UI-> PBX-> Basic/Call Routes-> VoIP Trunks.** Also, please configure their Inbound/Outbound routes accordingly.

2. Click edit button in the menu 

, and check if **Sync** LDAP **Enable** is selected, this option will allow UCM6510_A update remote LDAP server automatically from peer UCM6510_B. In addition, **Sync LDAP Password** must match for UCM6510_A and UCM6510_B in order to sync LDAP contact automatically. Port number can be anything between 0~65535, and use the outbound rule created in step 1 for the **LDAP Outbound Rule** option**.**

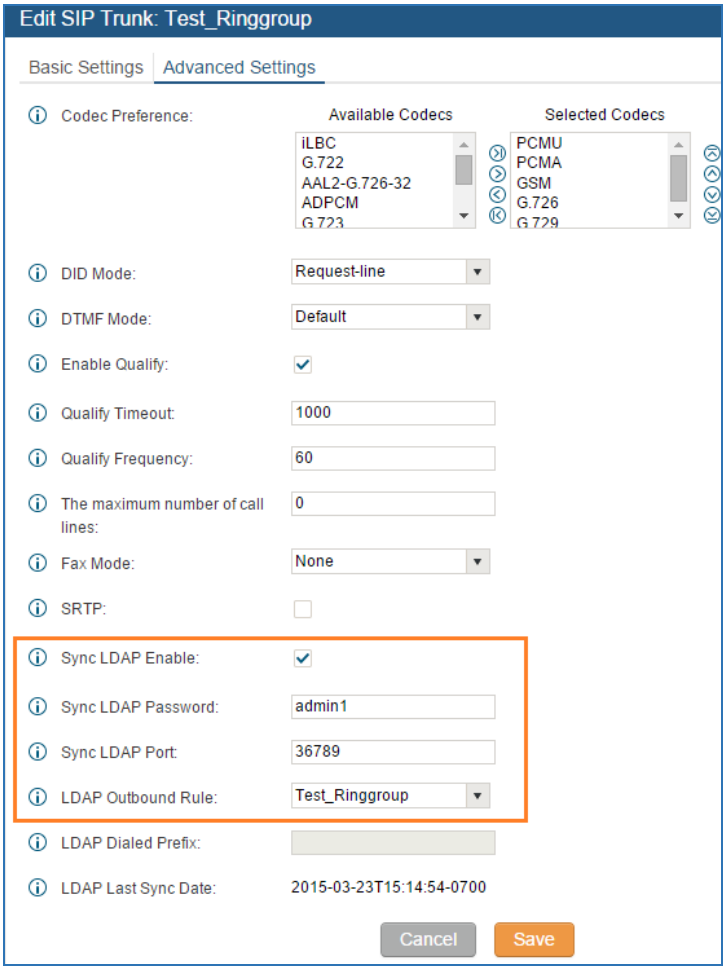


Figure 112: Sync LDAP Server option

3. In case if LDAP server doesn't sync automatically, user can manually sync LDAP server. Under **VoIP Trunks** page, click sync button shown in the following figure to manually sync LDAP contacts from peer UCM6510.

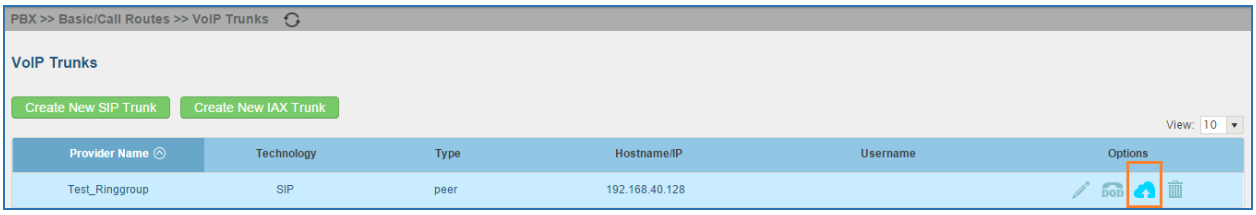


Figure 113: Manually Sync LDAP Server

4. Under **Ring Groups** setting page, click Create New Ring Group. **Ring Groups** can be found under web **UI-> PBX-> Call Features-> Ring Groups**.

5. If LDAP server is synced correctly, **Available LDAP Numbers** box will display available remote extensions that can be included in the current ring group. Please also make sure the extensions in the peer UCM6510 can be included into that UCM6510's LDAP contact.

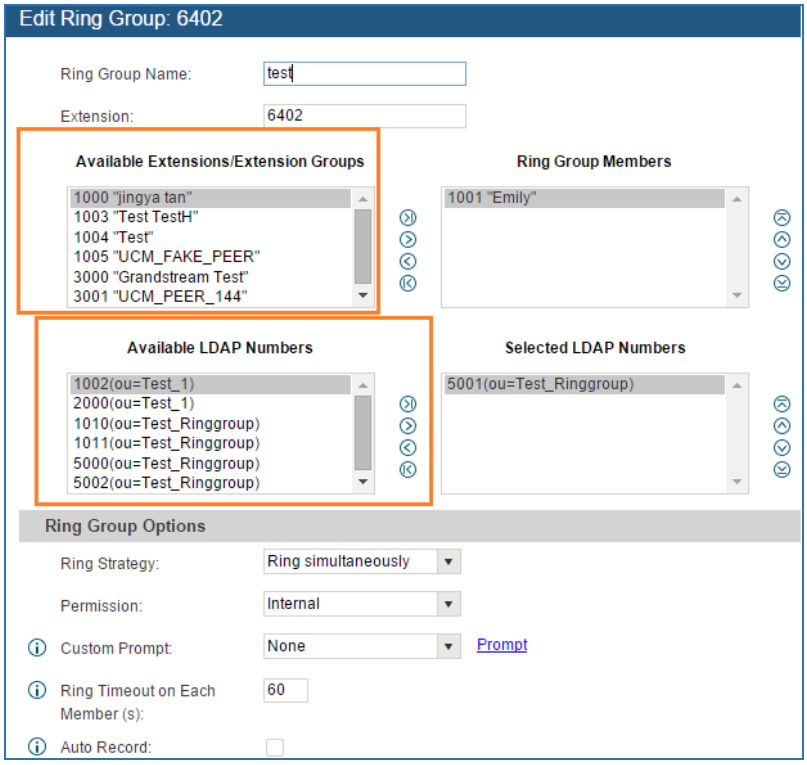


Figure 114: Ring Group Remote Extension

This page intentionally left blank

PAGING AND INTERCOM GROUP

Paging and Intercom Group can be used to make an announcement over the speaker on a group of phones. Targeted phones will not ring but answer immediately using speaker. The UCM6510 paging and intercom can be used via feature code to a single extension or a paging/intercom group. This sections describes the configuration of paging/intercom group under web GUI->**PBX**->**Call Features**->**Paging/Intercom**.

CONFIGURE PAGING/INTERCOM GROUP

- Click on "Create New Paging/Intercom Group" to add paging/intercom group.

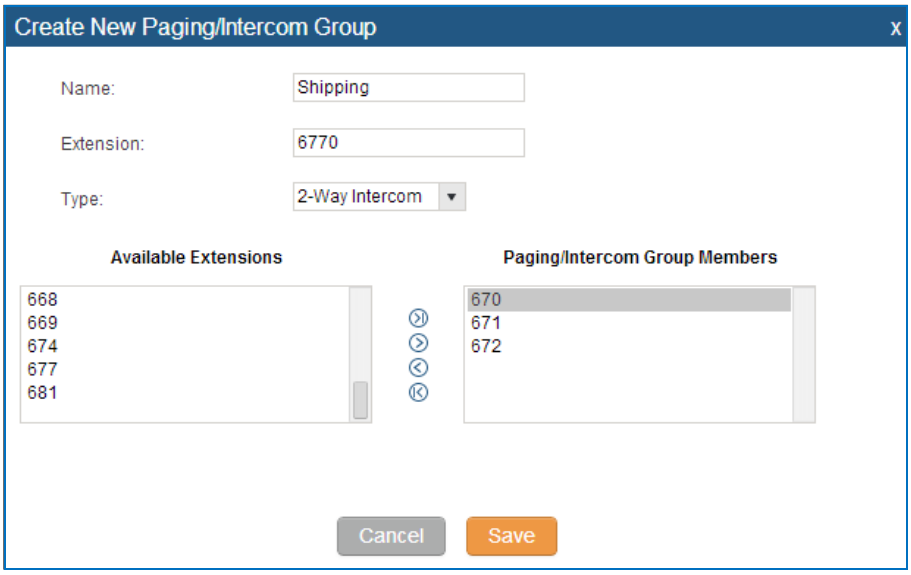


Figure 115: Paging/Intercom Group

Table 73: Paging/Intercom Group Configuration Parameters

Name	Configure paging/intercom group name.
Extension	Configure the paging/intercom group extension.
Type	Select "2-way Intercom" or "1-way Page".
Custom Prompt	This option is setting a custom prompt used as announcement placed to the person receiving a paging/internal call. The file can be uploaded from the **web GUI**->**Internal Options**->**Custom Prompt**, or click the 'Prompt' to add additional recorded.
Page/Intercom Group Members	Select available users from the left side to the paging/intercom group member list on the right.

- Click on to edit the paging/intercom group.
- Click on to delete the paging/intercom group.
- Click on "Paging/Intercom Group Settings" to edit Alert-Info Header. This header will be included in the SIP INVITE message sent to the callee in paging/intercom call.

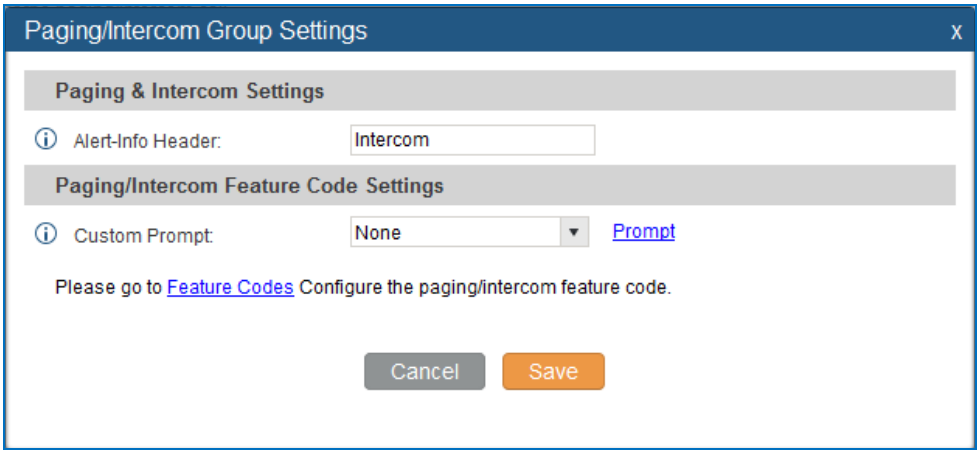


Figure 116: Page/Intercom Group Settings

- The UCM6510 has pre-configured paging/intercom feature code. By default, the Paging Prefix is *81 and the Intercom Prefix is *80. To edit page/intercom feature code, click on "Feature Codes" in the "Paging/Intercom Group Settings" dialog. Or users could go to web GUI->**PBX**->**Internal Options**->**Feature Codes** directly.

CALL QUEUE

The UCM6510 supports call queue by using static agents or dynamic agents. Call Queue system can accept more calls than the available agents. Incoming calls will be hold until next representative is available in the system. This sections describes the configuration of call queue under web GUI->**PBX**->**Call Features**->**Call Queue**.

CONFIGURE CALL QUEUE

Call queue settings can be accessed via web GUI->**PBX**->**Call Features**->**Call Queue**.

- Click on "Create New Queue" to add call queue.

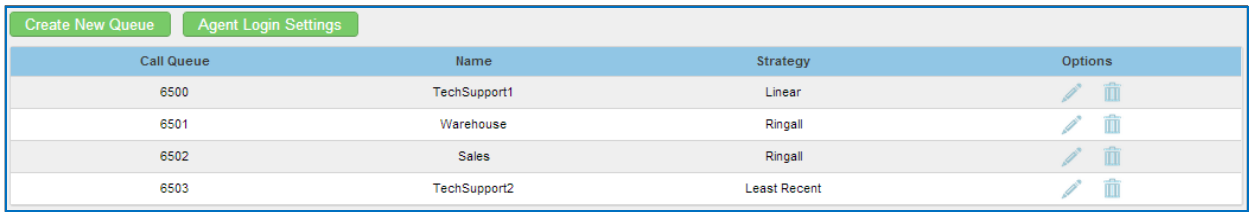


Figure 117: Call Queue

- Click on to edit the call queue. The call queue configuration parameters are listed in the table below.

Table 74: Call Queue Configuration Parameters

Extension	Configure the call queue extension.
Name	Configure the call queue name to identify the call queue.
Strategy	Select the strategy for the call queue. • Ring All Ring all available Agents simultaneously until one answers. • Linear Ring agents in the specified order. • Least Recent Ring the agent who has been called the least recently. • Fewest Calls Ring the agent with the fewest completed calls. • Random Ring a random agent. • Round Robin Ring the agents in Round Robin scheduling with memory.

	The default setting is "Ring All".
Music On Hold	Select the Music On Hold class for the call queue. **Note:** Music On Hold classes can be managed from web GUI-> **PBX**->**Internal Options**->**Music On Hold**.
Leave When Empty	Configure whether the callers will be disconnected from the queue or not if the queue has no agent anymore. The default setting is "Strict". • Yes Callers will be disconnected from the queue if all agents are paused or invalid. • No Never disconnect the callers from the queue when the queue is empty. • Strict Callers will be disconnected from the queue if all agents are paused, invalid or unavailable.
Dial in Empty Queue	Configure whether the callers can dial into a call queue if the queue has no agent. The default setting is "No". • Yes Callers can always dial into a call queue. • No Callers cannot dial into a queue if all agents are paused or invalid. • Strict Callers cannot dial into a queue if the agents are paused, invalid or unavailable.
Permission	Assign permission level to the user. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal".
Dynamic Login Password	If enabled, the configured PIN number is required for dynamic agent to log in. The default setting is disabled.
Ring Time Out	Configure the number of seconds an agent will ring before the call goes to the next agent. The default setting is 15 seconds.
Wrapup Time	Configure the number of seconds before a new call can ring the queue after the last call on the agent is completed. If set to 0, there will be no delay between calls to the queue. The default setting is 15 seconds.
Max Queue Length	Configure the maximum number of calls to be queued at once. This number does not include calls that have been connected with agents. It only includes calls not connected yet. The default setting is 0, which means

	unlimited. When the maximum value is reached, the caller will be treated with busy tone followed by the next calling rule after attempting to enter the queue.
Report Hold Time	If enabled, the UCM6510 will report (to the agent) the duration of time of the call before the caller is connected to the agent. The default setting is "No".
Wait Time	If enabled, users will be disconnected after the configured number of seconds. The default setting is "No". **Note:** It is recommended to configure "Wait Time" longer than the "Wrapup Time".
Auto Record	If this option is enabled, the calls using this extension or trunk will be automatically recorded.
Enable Destination	This option will enable destination for call queue. If it is enabled, Wait Time will be disabled.
Queue Timeout	Configure the global timeout (in seconds) of this call queue. It must be larger than the value of ring timeout. The call will be transferred to fail over destination directly if this time is exceeded.
Default Destination	The call would be routed to this destination if no one in this ring group answers the call. It can be set to Extension, Voicemail, Queues, Ring Group, Voicemail Group, IVR, and External Number.
Agents	Select the available users to be the static agents in the call queue. Choose from the available users on the left to the static agents list on the right. Click on to arrange the order.

- Click on to delete the call queue.
- Click on "Agent Login Settings" to configure Agent Login Extension Postfix and Agent Logout Extension Postfix. Once configured, users could log in the call queue as dynamic agent.

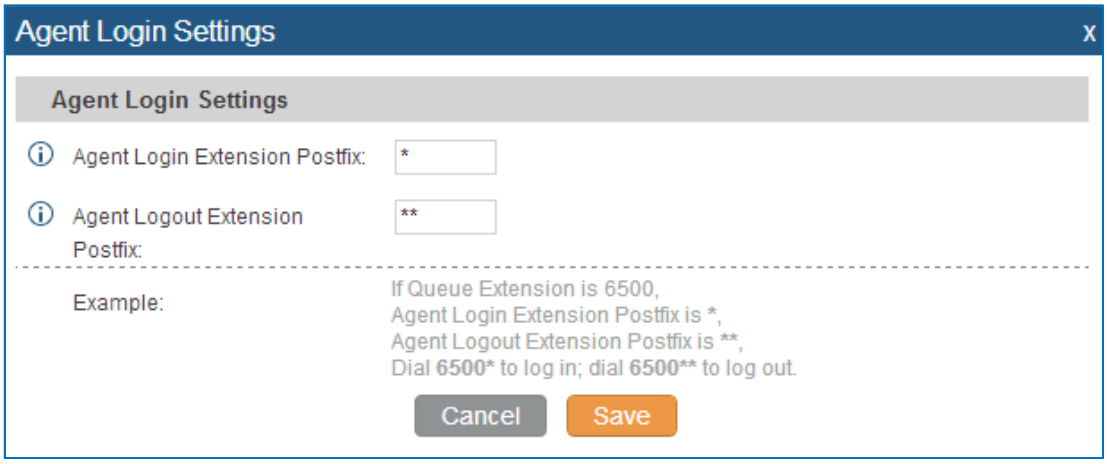


Figure 118: Agent Login Settings

For example, if the call queue extension is 6510, Agent Login Extension Postfix is * and Agent Logout Extension Postfix is **, users could dial 6510* to login to the call queue as dynamic agent and dial 6510** to logout from the call queue. Dynamic agent doesn't need to be listed as static agent and can log in/log out at any time.

- Call queue feature code "Agent Pause" and "Agent Unpause" can be configured under web GUI->**PBX**->**Internal Options**->**Feature Codes**. The default feature code is *83 for "Agent Pause" and *84 for "Agent Unpause".
- Queue recordings are shown on the Call Queue page. Click on to download the recording file in .wav format; click on to delete the recording file. To delete multiple recording files by one click, select several recording files to be deleted and click on “Delete Selected Recording Files” or click on “Delete All Recording Files” to delete all recording files.

EXTENSION GROUPS

The UCM6510 extension group feature allows users to assign extensions to different groups to better manage the configurations on the PBX. For example, when configuring "Enable Filter on Source Caller ID", users could select a group instead of each person's extension to assign. This feature simplifies the configuration process and helps manage and categorize the extensions for business environment.

CONFIGURE EXTENSION GROUPS

Extension group can be configured via web GUI->**PBX**->**Call Features**->**Extension Groups**.

- Click on "Create New Extension Group" to create a new extension group.
- Click on to edit the extension group.

  Select extensions from the list on the left side to the right side.

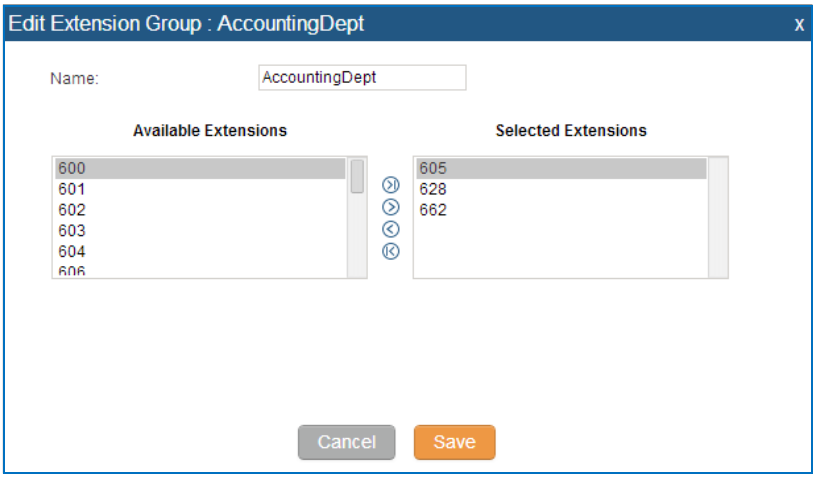


Figure 119: Edit Extension Group

- Click on to delete the extension group.

USE EXTENSION GROUPS

Here is an example where the extension group can be used. Go to web GUI->**PBX**->**Basic/Call Routes**->**Outbound Routes** and select "Enable Filter on Source Caller ID". Both single extensions and extension groups will show up for users to select.

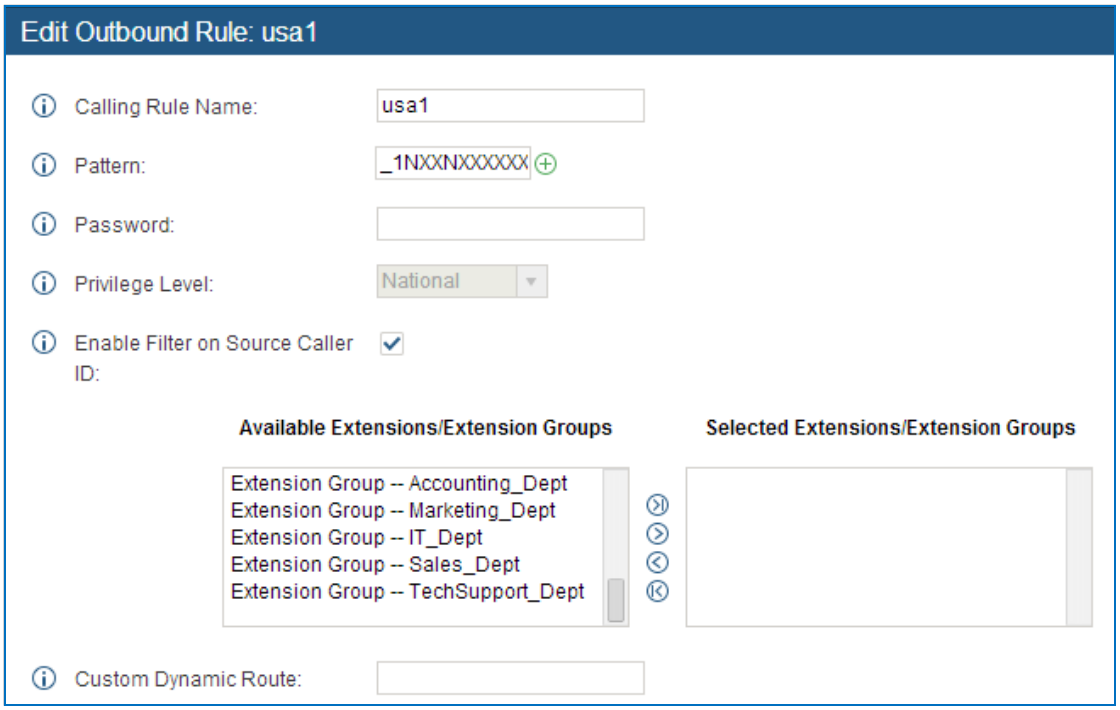


Figure 120: Select Extension Group in Outbound Route

PICKUP GROUPS

The UCM6510 supports pickup group feature which allows users to pick up incoming calls for other extensions if they are in the same pickup group, by dialing "Pickup Extension" feature code (by default *8).

CONFIGURE PICKUP GROUPS

Pickup groups can be configured via web GUI->**PBX**->**Call Features**->**Pickup Groups**.

- Click on "Create New Pickup Group" to create a new pickup group.
- Click on to edit the pickup group.

  Select extensions from the list on the left side to the right side.

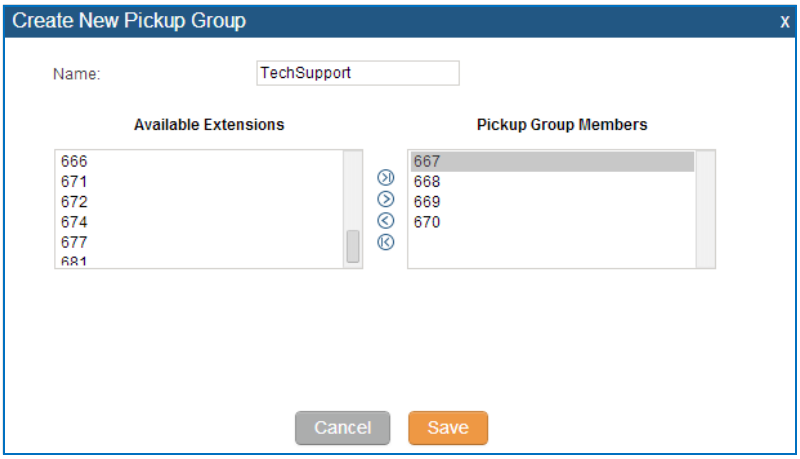


Figure 121: Edit Pickup Group

- Click on to delete the pickup group.

CONFIGURE PICKUP FEATURE CODE

When picking up the call for the pickup group member, the user only needs to dial the pickup feature code. It's not necessary to add the extension number after the pickup feature code. The pickup feature code is configurable under Web GUI->**PBX**->**Internal Options**->**Feature Codes**.

The default pickup feature code is *8.

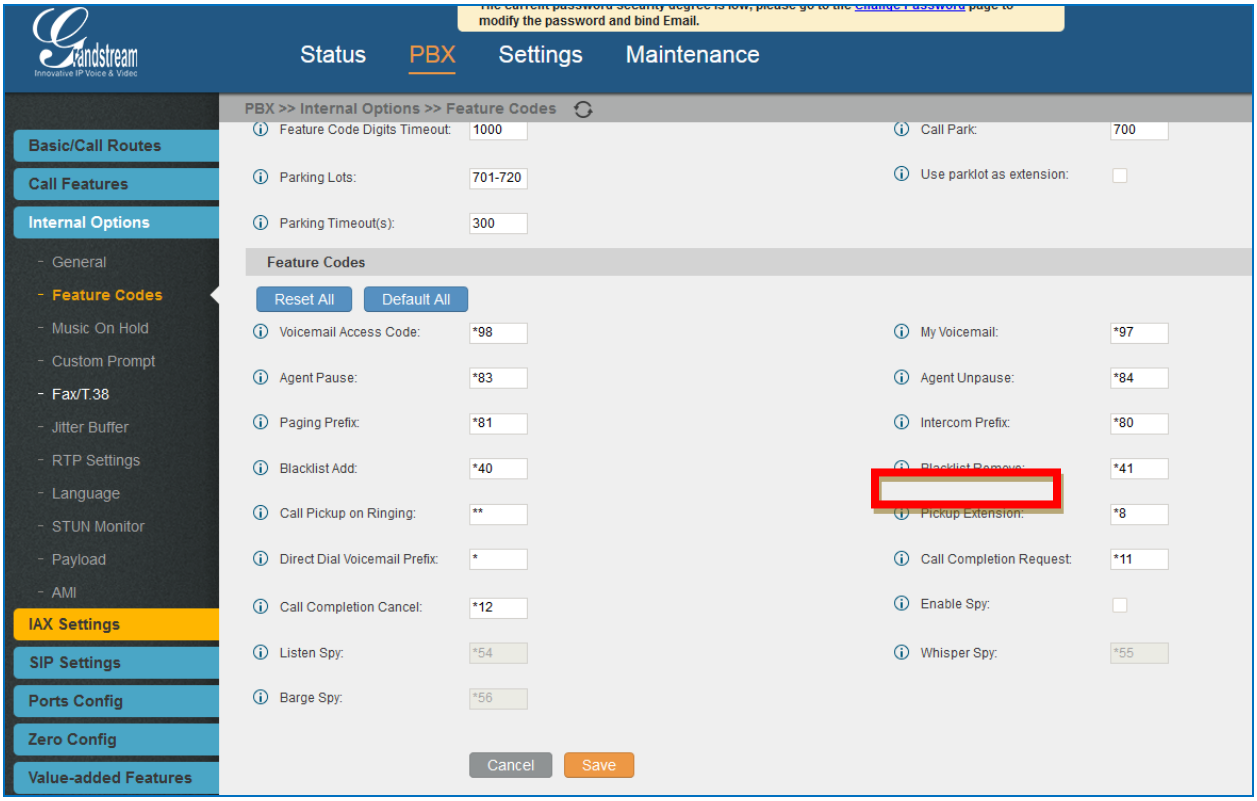


Figure 122: Edit Pickup Feature Code

MUSIC ON HOLD

Music On Hold settings can be accessed via web GUI->**PBX**->**Internal Options**->**Music On Hold**. In this page, users could configure music on hold class and upload music files. The "default" Music On Hold class already has 5 audio files defined for users to use.

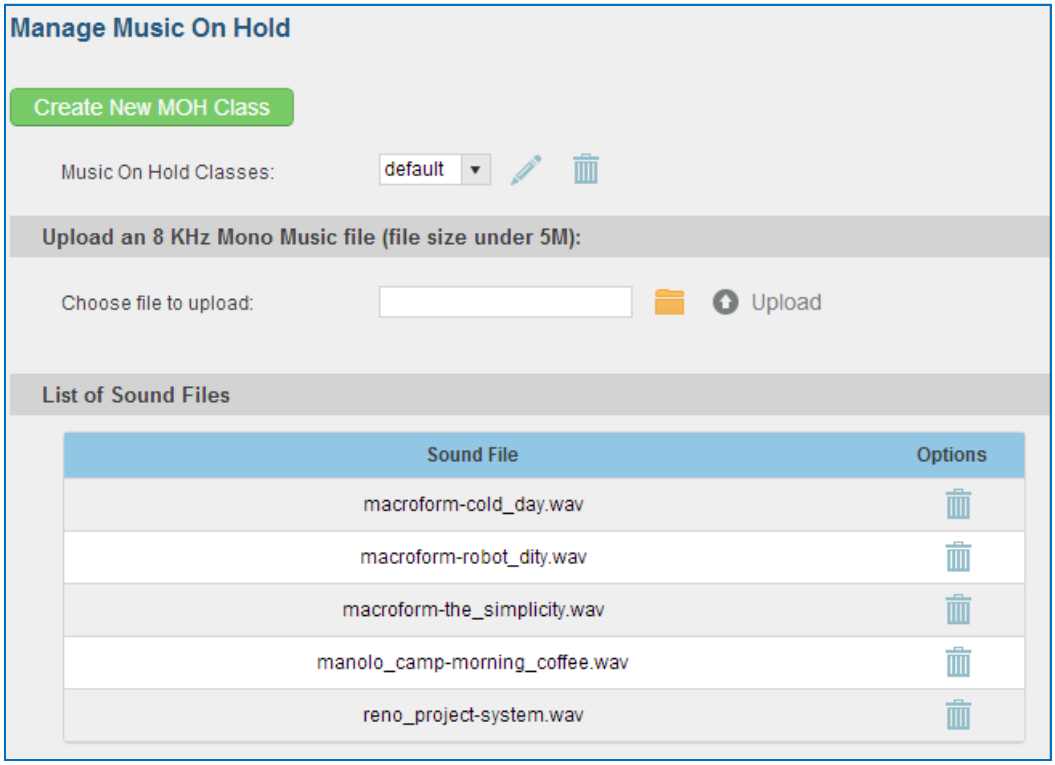


Figure 123: Music On Hold Default Class

- Click on "Create New MOH Class" to add a new Music On Hold class.
- Click on to configure the MOH class sort method to be "Alpha" or "Random" for the sound files.
- Click on next to the selected Music On Hold class to delete this Music On Hold class.
- Click on to select music file from local PC and click on to start uploading. The music file uploaded has to be 16 bit, 8 KHz Mono in .wav format with size smaller than 5M.
- Click on next to the sound file to delete it from the selected Music On Hold Class.

Note:

In case the users have deleted the system MOH files, there are two ways to recover.

1. Users could download the MOH file from this link:
   http://downloads.asterisk.org/pub/telephony/sounds/releases/asterisk-moh-opsound-wav-2.03.tar.gz
   After downloading, unzip the pack and upload the music files to the UCM6510.
2. Factory reset could also recover the MOH file on the UCM.

FAX/T.38

The UCM6510 supports T.30/T.38 Fax and Fax Pass-through. It can also convert the received Fax to PDF format and send it to the configured Email address. Fax/T.38 settings can be accessed via web GUI->**PBX**->**Internal Options**->**FAX/T.38**.

CONFIGURE FAX/T.38

- Click on "Create New Fax Extension". In the popped up window, fill the extension, name and Email address to send the received Fax to.
- Click on "Fax Settings" to configure the Fax parameters.

Table 75: FAX/T.38 Settings

Enable Error Correction Mode	Configure to enable Error Correction Mode (ECM) for the Fax. The default setting is "Yes".
Maximum Transfer Rate	Configure the maximum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14400. The default setting is 14400.
Minimum Transfer Rate	Configure the minimum transfer rate during the Fax rate negotiation. The possible values are 2400, 4800, 7200, 9600, 12000 and 14000. The default setting is 2400.
Default Email Address	Configure the Email address to send the received Fax to if user's Email address cannot be found. **Note:** The extension's Email address or the Fax's default Email address needs to be configured in order to receive Fax from Email. If neither of them is configured, Fax will be not be received from Email.
Template Variables	Fill in the "Subject:" and "Message:" content, to be used in the Email when sending the Fax to the users. The template variables are: • ${CALLERIDNUM} : Caller ID Number • ${CALLERIDNAME} : Caller ID Name • ${RECEIVEEXTEN} : The extension to receive the Fax • ${FAXPAGES} : Number of pages in the Fax • ${VM_DATE} : The date and time when the Fax is received

- Click on to edit the Fax extension.
- Click on to delete the Fax extension.

SAMPLE CONFIGURATION TO RECEIVE FAX FROM PSTN LINE

The following instructions describe how to use the UCM6510 to receive Fax from PSTN line on the Fax machine connected to the UCM6510 FXS port.

1. Connect Fax machine to the UCM6510 FXS port.
2. Connect PSTN line to the UCM6510 FXO port.
3. Go to web GUI->**PBX**->**Analog Trunks** page.
4. Create or edit the analog trunk for Fax as below.

   Fax Detection: Make sure "Fax Detection" option is set to "No".

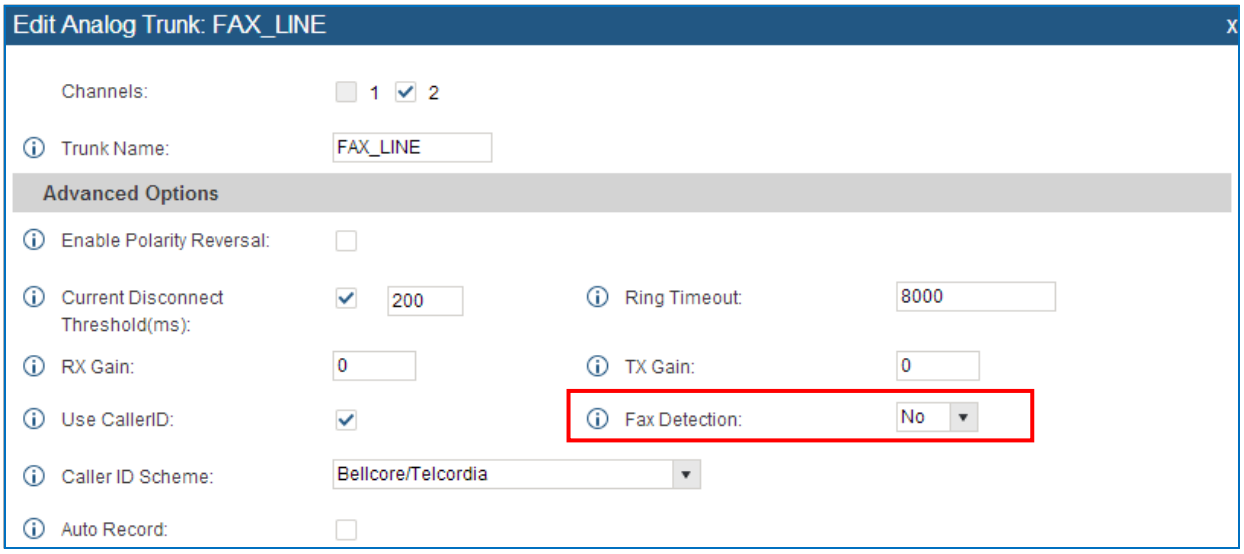


Figure 124: Configure Analog Trunk without Fax Detection

5. Go to UCM6510 web GUI->**PBX**->**Basic/Call Routes**->**Extensions** page.
6. Create or edit the extension for FXS port.

   - **Analog Station**: Select FXS port to be assigned to the extension. By default, it's set to "None".
   - Once selected, analog related settings for this extension will show up in "**Analog Settings**" section.

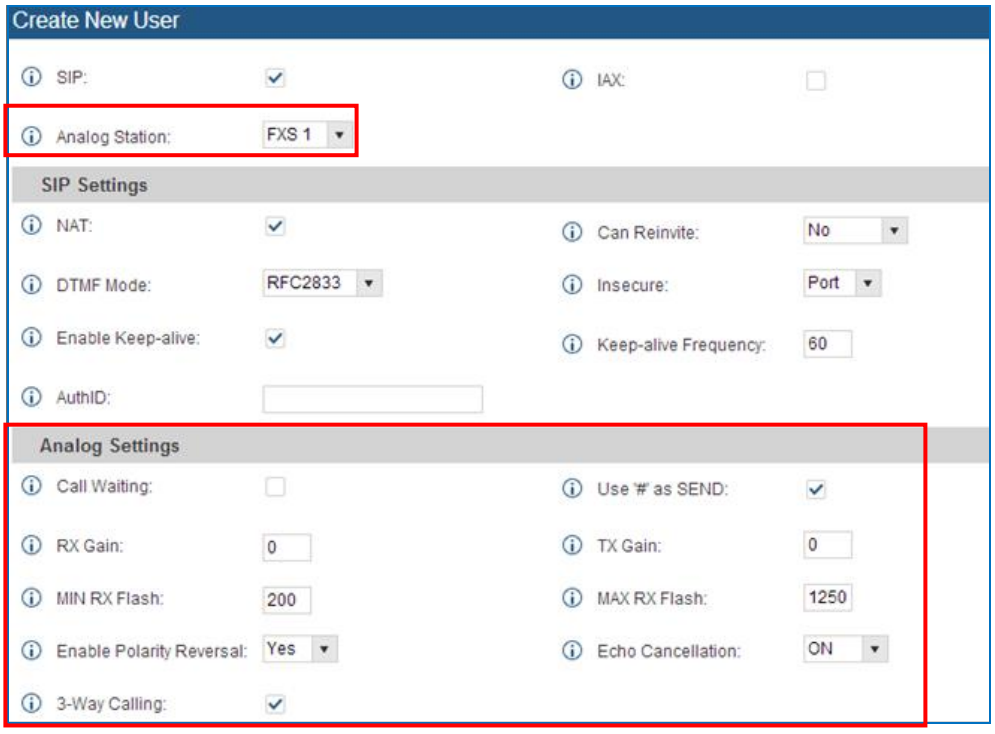


Figure 125: Configure Extension For Fax Machine

7. Go to web GUI->**PBX**->**Basic/Call Routes**->**Inbound Routes** page.
8. Create an inbound route to use the Fax analog trunk. Select the created extension for Fax machine in step 4 as the default destination.

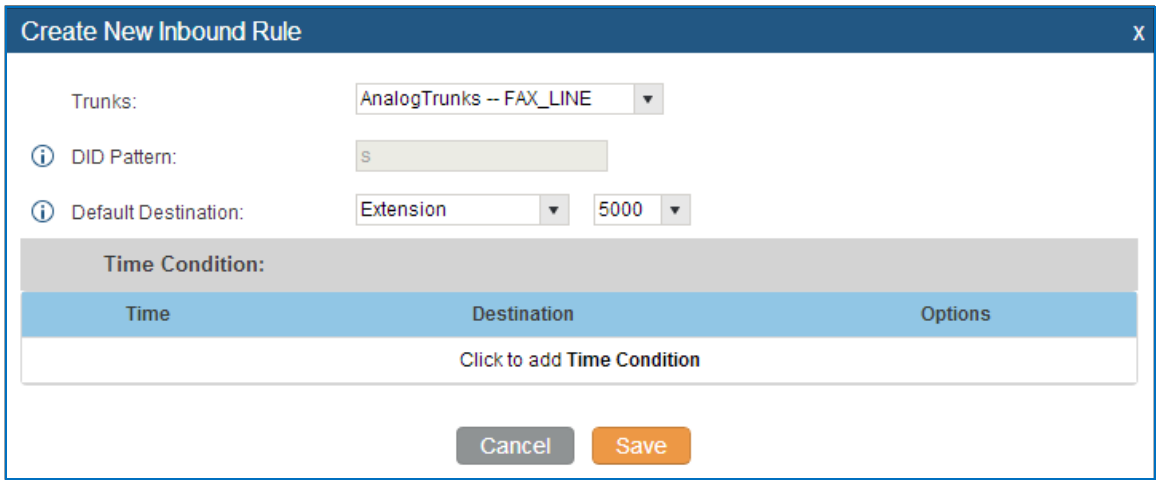


Figure 126: Configure Inbound Rule for Fax

Now the Fax configuration is done. When there is an incoming Fax calling to the PSTN number for the FXO port, it will send the Fax to the Fax machine.

SAMPLE CONFIGURATION FOR FAX-TO-EMAIL

The following instructions describe a sample configuration on how to use Fax-to-Email feature on the UCM6510.

1. Connect PSTN line to the UCM6510 FXO port.
2. Go to UCM6510 web GUI->**Internal Options**->**Fax/T.38** page. Create a new Fax extension.

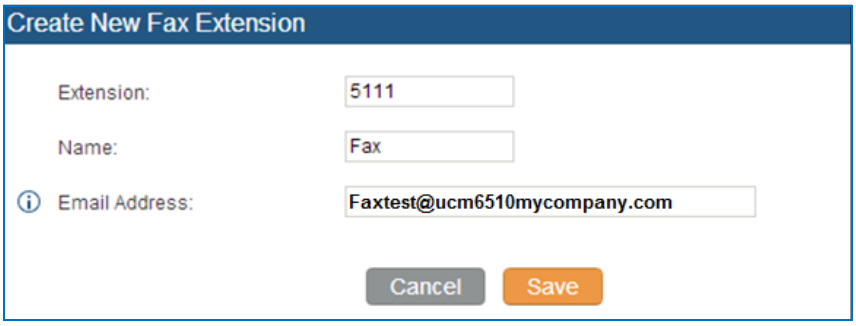


Figure 127: Create Fax Extension

3. Go to UCM6510 web GUI->**Basic/Call Routes**->**Analog Trunks** page. Create a new analog trunk with "FAX Detection" set to "No".
4. Go to UCM6510 web GUI->**Basic/Call Routes**->**Inbound Routes** page. Create a new inbound route and set the default destination to the Fax extension.

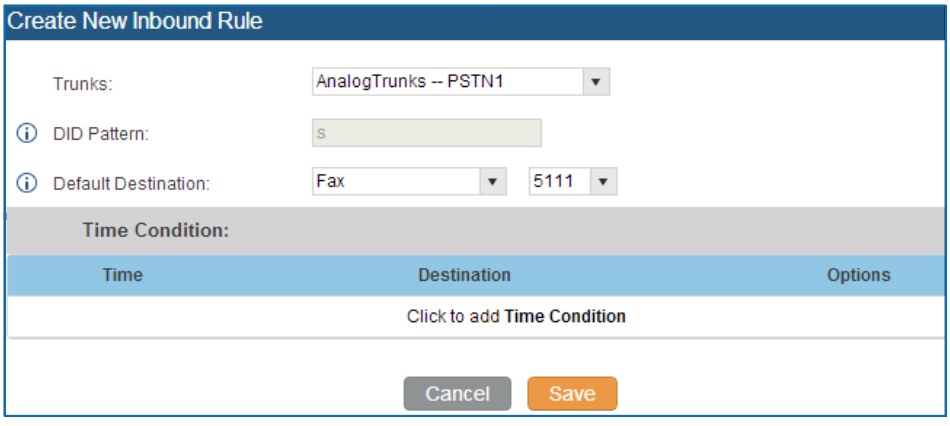


Figure 128: Inbound Route to Fax Extension

5. Once successfully configured, the incoming Fax from external Fax machine to the PSTN line number will be converted to PDF file and sent to the Email address **Faxtest@ucm6510mycompany.com** as attachment.

ASTERISK MANAGER INTERFACE (RESTRICTED ACCESS)

Starting from firmware 1.0.1.10, the UCM6510 supports Asterisk Manager Interface (AMI) with restricted access. AMI allows a client program to connect to an Asterisk instance commands or read events over a TCP/IP stream. It's particularly useful when the system admin tries to track the state of a telephony client inside Asterisk.

User could configure AMI parameters on UCM6510 web GUI->**PBX**->**Internal Options**->**AMI**. For details on how to use AMI on UCM6510, please refer to the following AMI guide:

http://www.grandstream.com/products/ucm_series/ucm61xx/documents/ucm6100_ami_guide.pdf

---

⚠ **Warning:**

Please do not enable AMI on the UCM6510 if it is placed on a public or untrusted network unless you have taken steps to protect the device from unauthorized access. It is crucial to understand that AMI access can allow AMI user to originate calls and the data exchanged via AMI is often very sensitive and private for your UCM6510 system. Please be cautious when enabling AMI access on the UCM6510 and restrict the permission granted to the AMI user. By using AMI on UCM6510 you agree you understand and acknowledge the risks associated with this.

This page intentionally left blank

FOLLOW ME

Follow Me is a feature on the UCM6510 that allows users to direct calls to other phone numbers and have them ring all at once or one after the other. Calls can be directed to users' home phone, office phone, mobile and etc. The calls will get to the user no matter where they are. Follow Me option can be found under web **GUI-> PBX-> Call Features-> Follow Me.**

To configure follow me:

1. Click on "Create New Follow Me" and then select an extension to be configured with Follow Me.

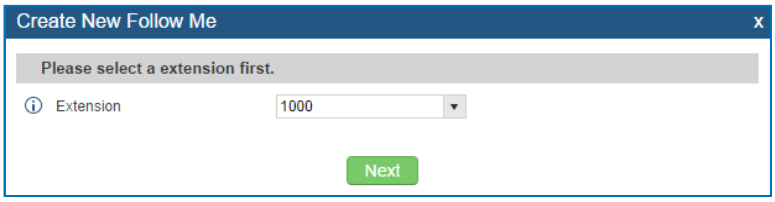


Figure 129: Create Follow Me

2. Click on "Next" to continue editing Follow Me configuration.

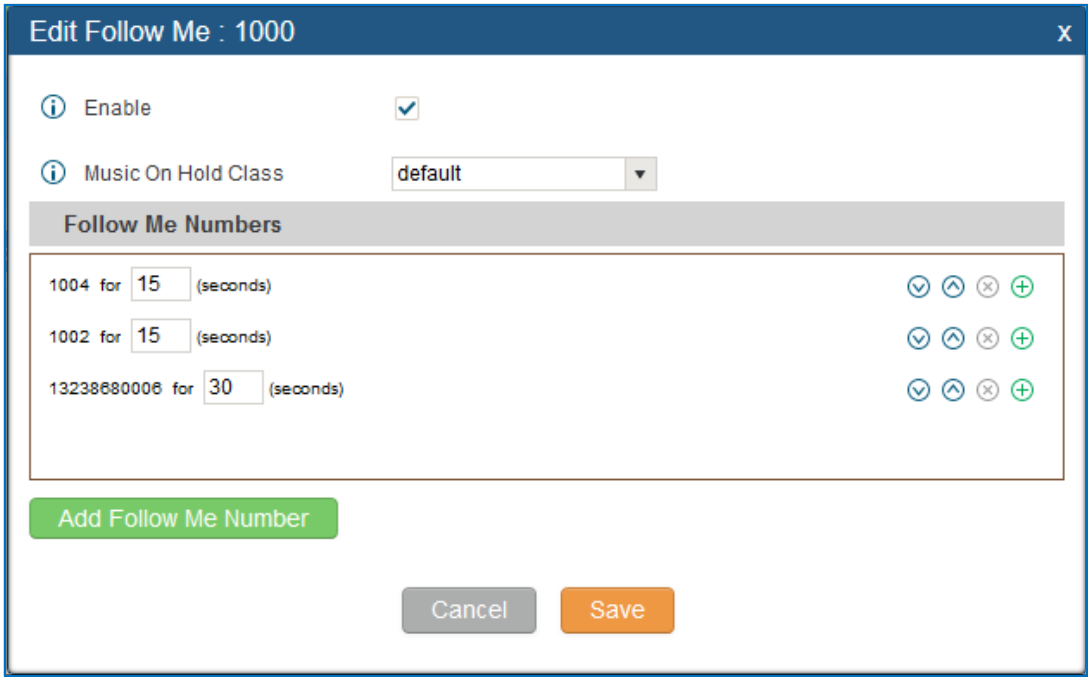


Figure 130: Edit Follow Me

3. Click on “Add Follow Me Number” to add local extensions or external numbers to be called after ringing the extension selected in the first step.
4. Once created, it will be displayed on the follow me web page list. Click on to edit the Follow Me configuration. Click on to delete the Follow Me.

The following table shows the Follow Me configuration parameters.

Table 76: Follow Me Settings

Enable	Configure to enable or disable Follow Me for this user.
Skip Trunk Auth	If external number is added in the Follow Me, please make sure this option is enabled or the “Skip Trunk Auth” option of the extension is enabled, otherwise the external Follow Me number cannot be reached.
Music On Hold Class	Configure the Music On Hold class that the caller would hear while tracking the user.
Confirm When Answering	By default it is enabled and user will be asked to press 1 to accept the call or to press 2 to reject the call after answering a Follow Me call. If it is disabled, the Follow Me call will be established once after the user answers it.
Follow Me Numbers	The added numbers are listed here. Click on to arrange the order. Click on to delete the number. Click on to add new numbers.
New Follow Me Number	Add a new Follow Me number which could be a ‘Local Extension’ or ‘External Number’. The selected dial plan should have permissions to dial the defined external number.
Dialing Order	Select the order in which the Follow Me destinations will be dialed to reach the user: ring all at once or ring one after the other.

5. Click on “Follow Me Options” to enable or disable the options listed in the following table.

Table 77: Follow Me Options

Playback Incoming Status Message	If enabled, the PBX will playback the incoming status message before starting the Follow Me steps.
Record the Caller’s Name	If enabled, the PBX will record the caller’s name from the phone so it can be announced to the callee in each step.
Playback Unreachable Status Message	If enabled, the PBX will playback the unreachable status message to the caller if the callee cannot be reached.

ONE-KEY DIAL

The UCM6510 supports One-Key Dial that allows users to call a certain destination by pressing one digit 0 to 9 on the keypad. This creates a system-wide speed dial access for all the extensions on the UCM6510.

To enable One-Key Dial, on the UCM6510 web GUI, go to page **PBX->Call Features->One-Key Dial**.

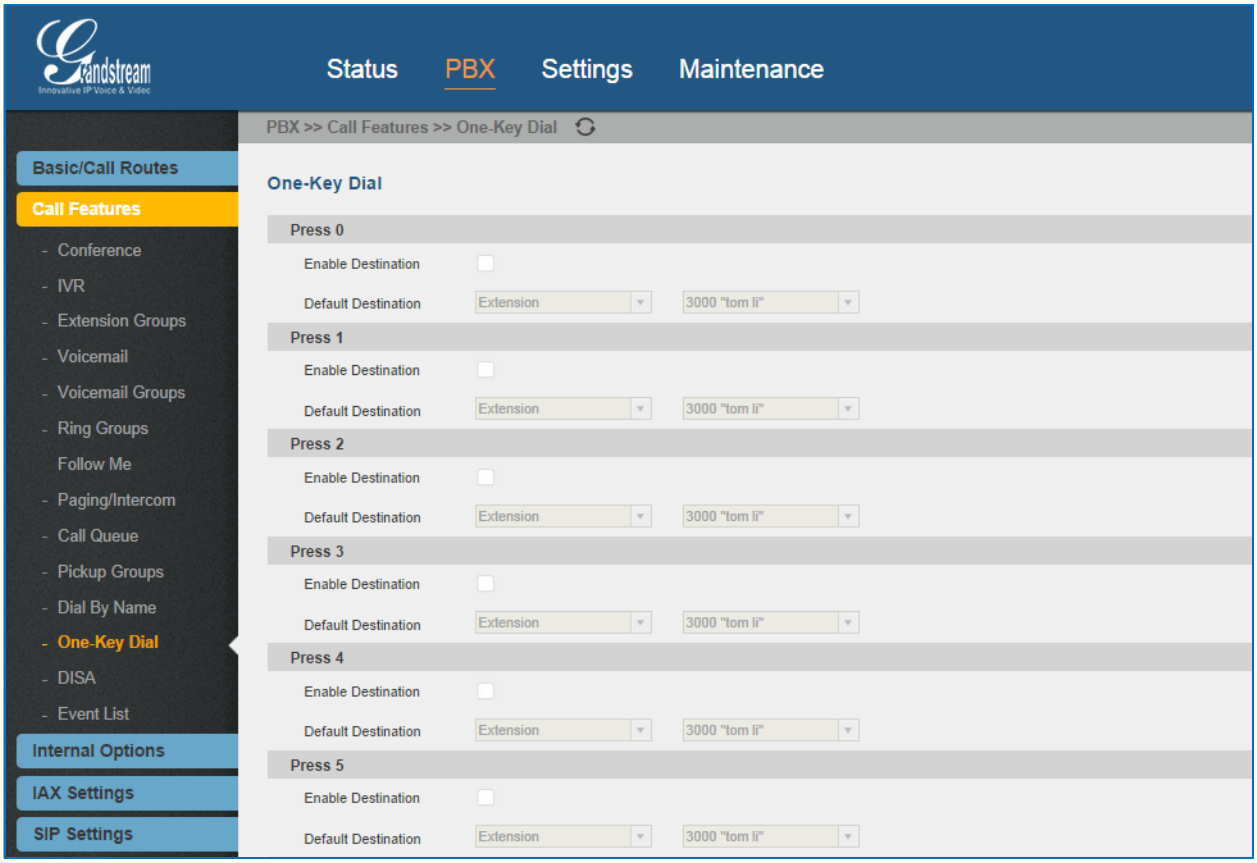


Figure 131: Configure One-Key Dial

User should first decide a digit used for One-Key Dial and check the option “Enable Destination” for the digit. Then select a dial destination from “Default Destination”. The supported destinations include extension, voicemail, conference room, voicemail group, IVR, ring group, call queue, page group, fax, DISA, Dial by Name and external number.

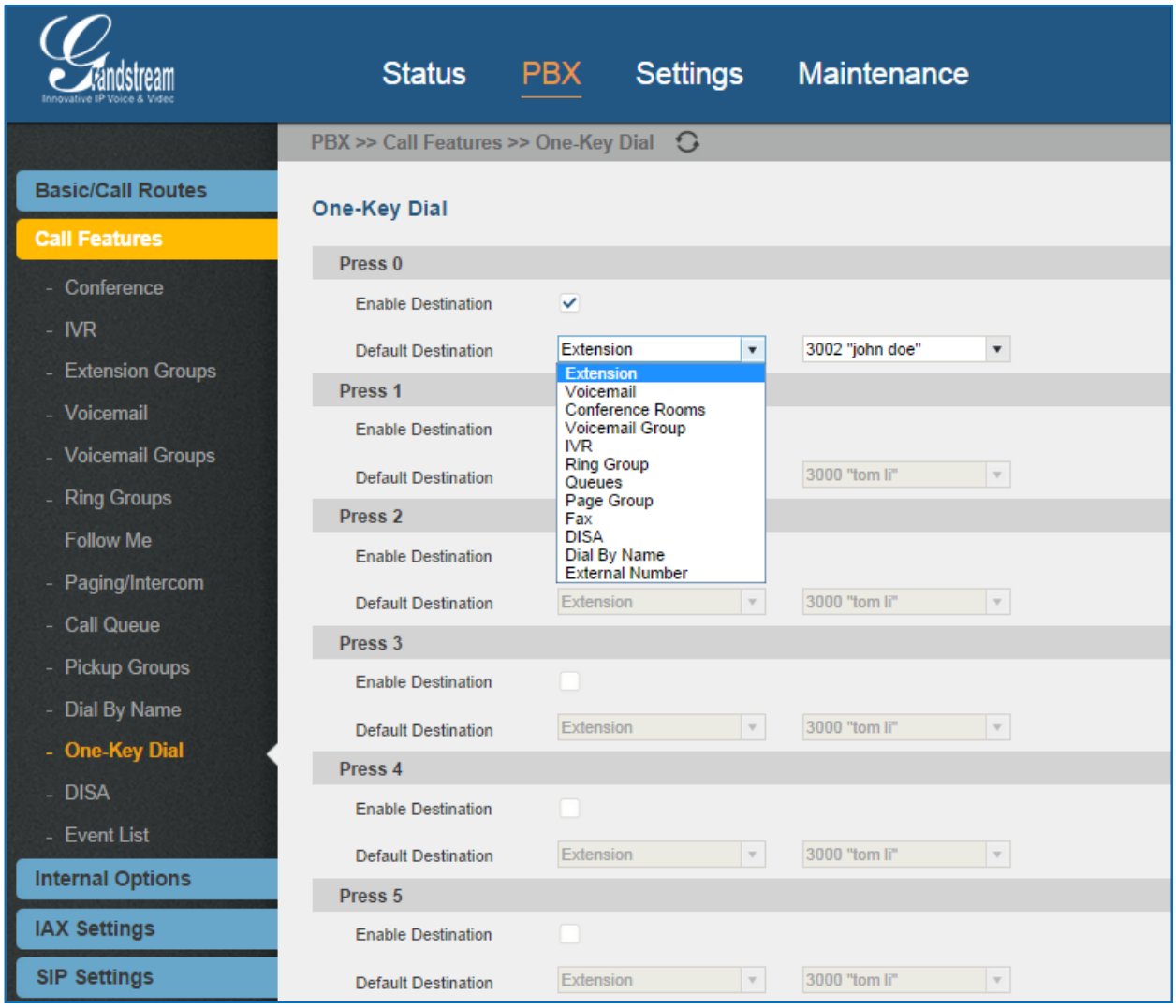


Figure 132: One-Key Dial Destinations

DISA

In many situations the user will find the need to access his own IPPBX resources but he is not physically close to any one of his extensions. However, he does has access to his own cell phone. In this case we can use what is commonly known as DISA (Direct Inward System Access). Under this scenario, the user will be able to call from the outside first, whether it's using his cell phone, pay phone, regular PSTN and etc, and then call into a SIP trunk or PSTN trunk connected to UCM6510 as it is an internal extension.

The UCM6510 supports DISA to be used in IVR or inbound route. Before using it, create new DISA under web GUI->**Call Features**->**DISA**.

- Click on "Create New DISA" to add a new DISA.
- Click on to edit the DISA configuration.
- Click on to delete the DISA.

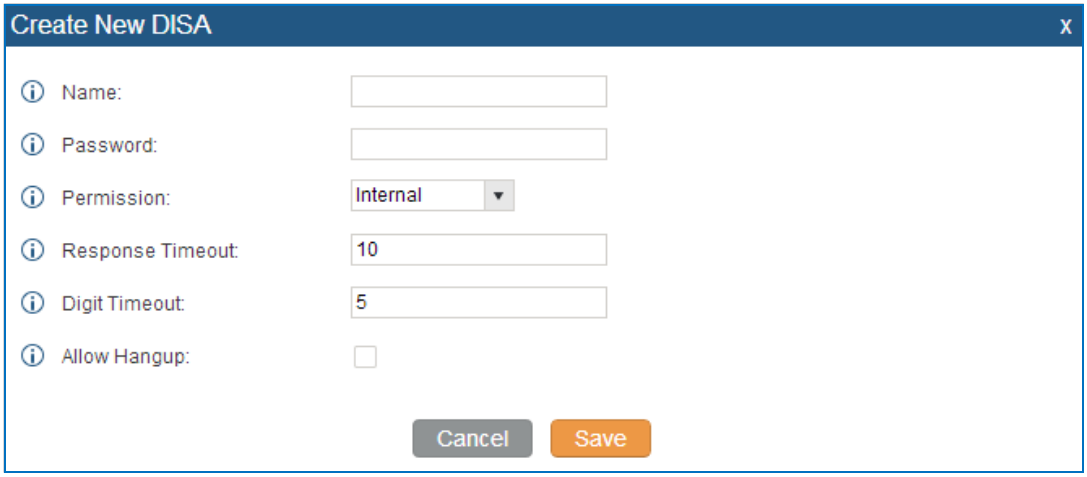


Figure 133: Create New DISA

Table 78: DISA Settings

Name	Configure DISA name to identify the DISA.
Password	Configure the password (digit only) required for the user to enter before using DISA to dial out. **Note:** The password has to be at least 4 digits.

Permission	Configure the permission level for DISA. The available permissions are "Internal", "Local", "National" and "International" from the lowest level to the highest level. The default setting is "Internal". If the user tries to dial outbound calls after dialing into the DISA, the UCM6510 will compared the DISA's permission level with the outbound route's privilege level. If the DISA's permission level is higher than (or equal to) the outbound route's privilege level, the call will be allowed to go through.
Response Timeout	Configure the maximum amount of time the UCM6510 will wait before hanging up if the user dials an incomplete or invalid number. The default setting is 10 seconds.
Digit Timeout	Configure the maximum amount of time permitted between digits when the user is typing the extension. The default setting is 5 seconds.
Allow Hangup	If enabled, during an active call, users can enter the UCM6510 hangup feature code (*0 by default) to disconnect the call or hang up directly. A new dial tone will be heard shortly for the user to make a new call. The default setting is "No".

Once successfully created, users can configure the inbound route destination as "DISA" or IVR key event as "DISA". When dialing into DISA, users will be prompted with password first. After entering the correct password, a second dial tone will be heard for the users to dial out.

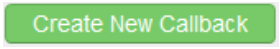
CALLBACK FEATURE

Callback is mainly designed for users who often use their mobile phones to make long distance or international calls which may have high service charges. The callback feature provides an economic solution for reduce the cost from this.

The callback feature works as follows:

1. Configure a new callback on the UCM6510.
2. On the UCM6510, configure destination of the inbound route for analog trunk to callback.
3. Save and apply the settings.
4. The user calls the PSTN number of the UCM6510 using the mobile phone, which goes to callback destination as specified in the inbound route.
5. Once the user hears the ringback tone from the mobile phone, hang up the call on the mobile phone.
6. The UCM6510 will call back the user.
7. The user answers the call.
8. The call will be sent to DISA or IVR which directs the user to dial the destination number.
9. The user will be connected to the destination number.

In this way, the calls are placed and connected through trunks on the UCM6510 instead of to the mobile phone directly. Therefore, the user will not be charged on mobile phone services for long distance or international calls.

To configure callback on the UCM6510, go to web GUI->**PBX**->**Call Features**->**Callback** page and click on 

. Configuration parameters are listed in the following table.

Table 79: Callback Configuration Parameters

Name	Configure a name to identify the Callback.
CallerID Pattern	Configure the pattern of the callers allowed to use this callback. The caller who places the inbound call needs to have the callerID match this pattern so that the caller can get callback after hanging up the call. **Note:** If leaving as blank, all numbers are allowed to use this callback.
Outbound Prepend	Configure the prepend digits to be added at before dialing the outside number. The number with prepended digits will be used to match the outbound route. '-' is the connection character which will be ignored.

Delay Before Callback	Configure the number of seconds to be delayed before calling back the user.
Destination	Configure the destination which the callback will direct the caller to. Two destinations are available: • IVR • DISA The caller can then enter the desired number to dial out via UCM6510 trunk.

BLF AND EVENT LIST

BLF

The UCM6510 supports BLF monitoring for extensions, ring group, call queue, conference room and parking lot. For example, on the user's phone, configure the parking lot number 701 as the BLF monitored number. When there is a parked call on 701, the LED for this BLF key will light up in red, meaning a call is parked against this parking lot. Pressing this BLF key can pick up the call from this parking lot.

⚠ **Note:**

- On the Grandstream GXP phones, the MPK supports "Call Park" mode, which is normally used to park the call by configuring the MPK number as call park feature code (e.g., 700). Users could also use "Call Park" mode to monitor and pick up the call on this parking lot by configuring the MPK number as parking lot number (e.g., 701).

EVENT LIST

Besides BLF, users can also configure the phones to monitor event list. By using event list, local extensions on the same UCM6510 or remote extensions on the VOIP trunk can be monitored. The event list settings is under web GUI->**Call Features**->**Event List**.

- Click on "Create New Event List" to add a new event list.
- Click on to edit the event list configuration.
- Click on to delete the event list.

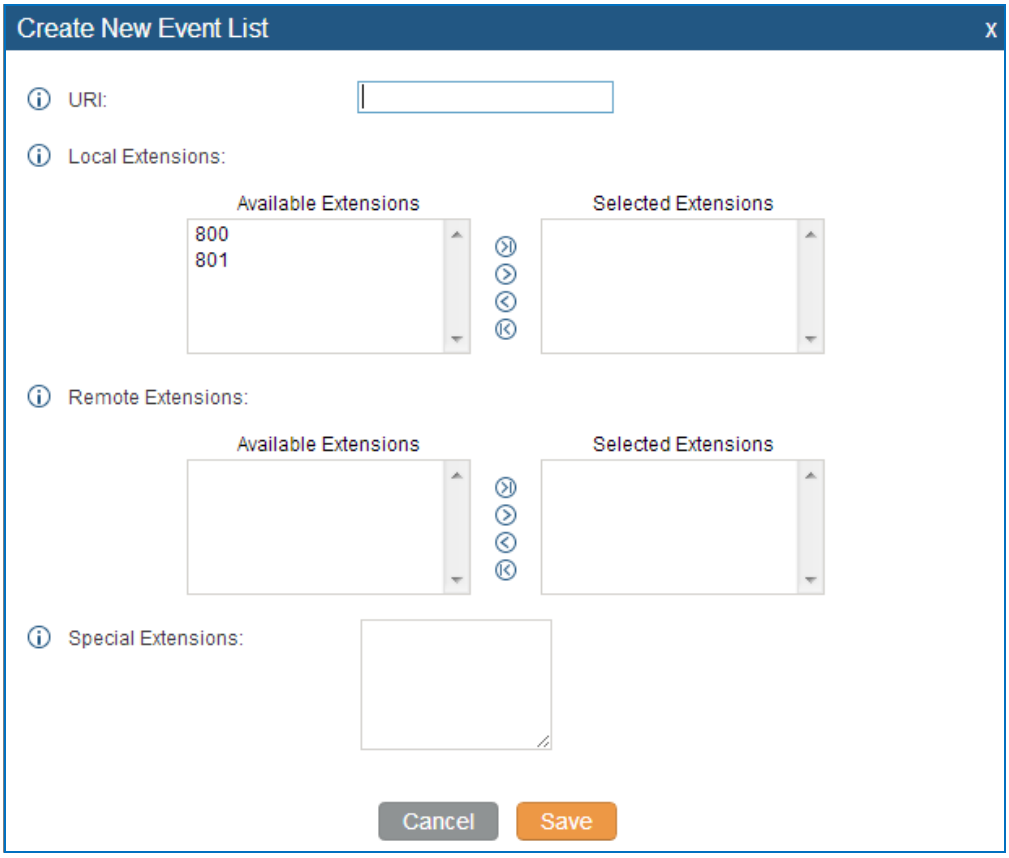


Figure 134: Create New Event List

Table 80: Event List Settings

URI	Configure the name of this event list (for example, office_event_list). Please note the URI name cannot be the same as the extension name on the UCM6510. The valid characters are letters, digits, _ and -.
Local Extensions	Select the available extensions listed on the local UCM6510 to be monitored in the event list.
Remote Extensions	If LDAP sync is enabled between the UCM6510 and the peer UCM6510, the remote extensions will be listed under "Available Extensions". If not, manually enter the remote extensions under "Special Extensions" field.
Special Extensions	Manually enter the remote extensions in the peer/register trunk to be monitored in the event list. Valid format: 5000,5001,9000

Remote extension monitoring works on the UCM6510 via event list BLF, among Peer SIP trunks or Register SIP trunks (register to each other). Therefore, please properly configure SIP trunks on the

UCM6510 first before using remote BLF feature. Please note the SIP end points need support event list BLF in order to monitor remote extensions.

When an event list is created on the UCM6510 and remote extensions are added to the list, the UCM6510 will send out SIP SUBSCIRBE to the remote UCM6510 to obtain the remote extension status. When the SIP end points registers and subscribes to the local UCM6510 event list, it can obtain the remote extension status from this event list.

Once successfully configured, the event list page will show the status of total extension and subscribers for each event list. Users can also select the event URI to check the monitored extension's status and the subscribers' details.

⚠ **Note:**

- To configure LDAP sync, please go to UCM6510 web GUI->**PBX**->**Basic/Call Routes**->**VoIP Trunk**. You will see "Sync LDAP Enable" option. Once enabled, please configure password information for the remote peer UCM6510 to connect to the local UCM6510. Additional information such as port number, LDAP outbound rule, LDAP Dialed Prefix will also be required. Both the local UCM6510 and remote UCM6510 need enable LDAP sync option with the same password for successful connection and synchronization.
- Currently LDAP sync feature only works between two UCM6510s.
- (Theoretically) Remote BLF monitoring will work when the remote PBX being monitored is non-UCM6510 PBX. However, it might not work the other way around depending on whether the non-UCM6510 PBX supports event list BLF or remote monitoring feature.

This page intentionally left blank

DIAL BY NAME

Dial By Name is a feature on the PBX that allows caller to search a person by first or last name via his/her phone's keypad. The administrator can define the Dial By Name directory including the desired extensions in the directory and the searching type by "first name" or "last name". After dialing in, the PBX IVR/Auto Attendant will guide the caller to spell the digits to find the person in the Dial By Name directory. This feature allows customers/clients to use the guided automatic system to get in touch with the enterprise employees without having to know the extension number, which brings convenience and improves business image for the enterprise.

DIAL BY NAME CONFIGURATION

The administrators can create the dial by name group under web GUI->**PBX**->**Call Features**->**Dial By Name**.

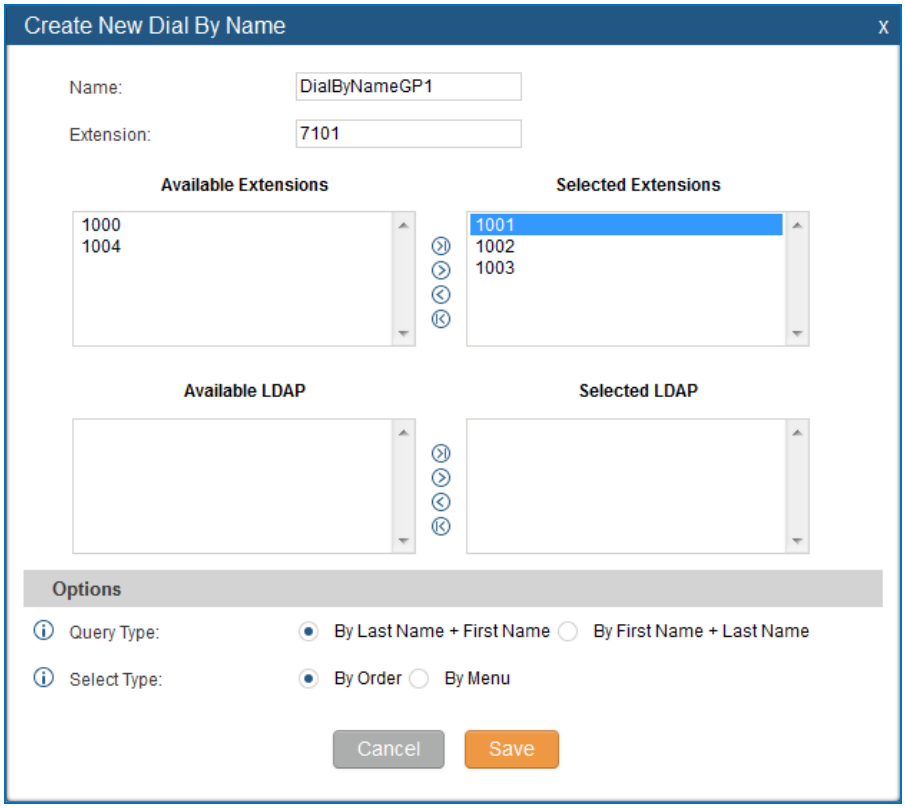


Figure 135: Create Dial By Name Group

1. **Group Name**

   Enter the Group Name. This is to identify the Dial By Name group. The Dial By Name group can be

used as the destination for inbound route and key pressing event for IVR. The group name defined here will show up in the destination list when configuring IVR and inbound route.

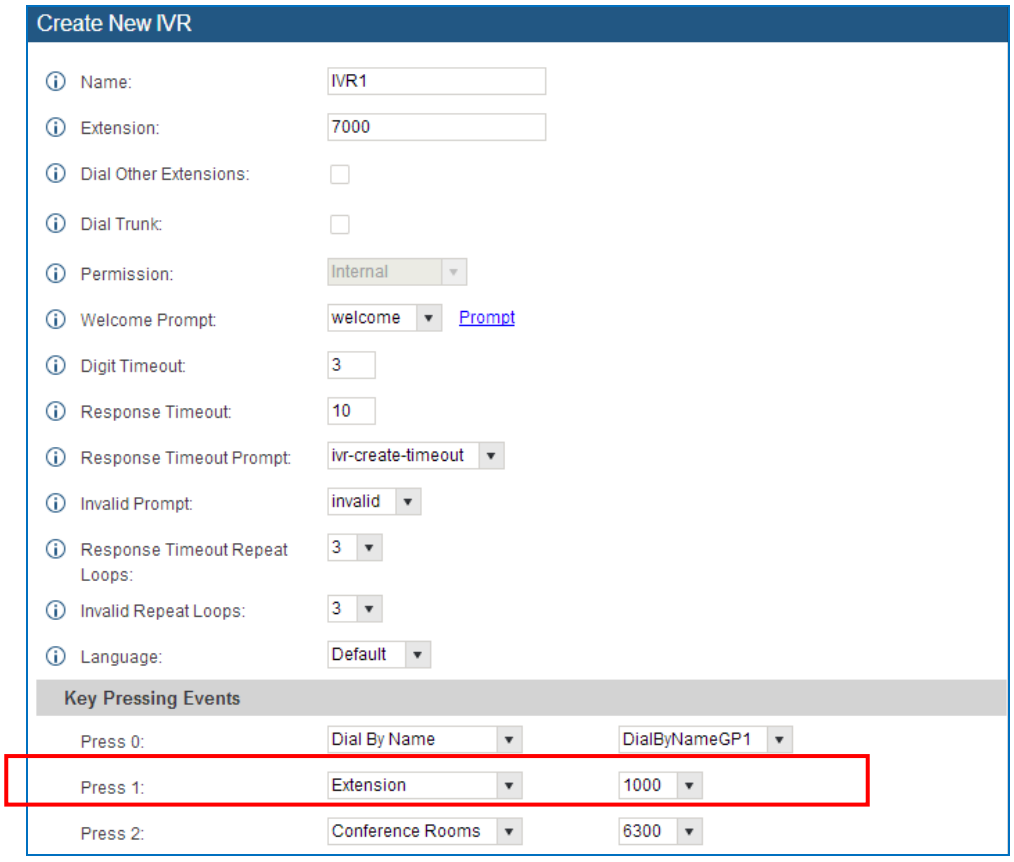


Figure 136: Dial By Name Group In IVR Key Pressing Events

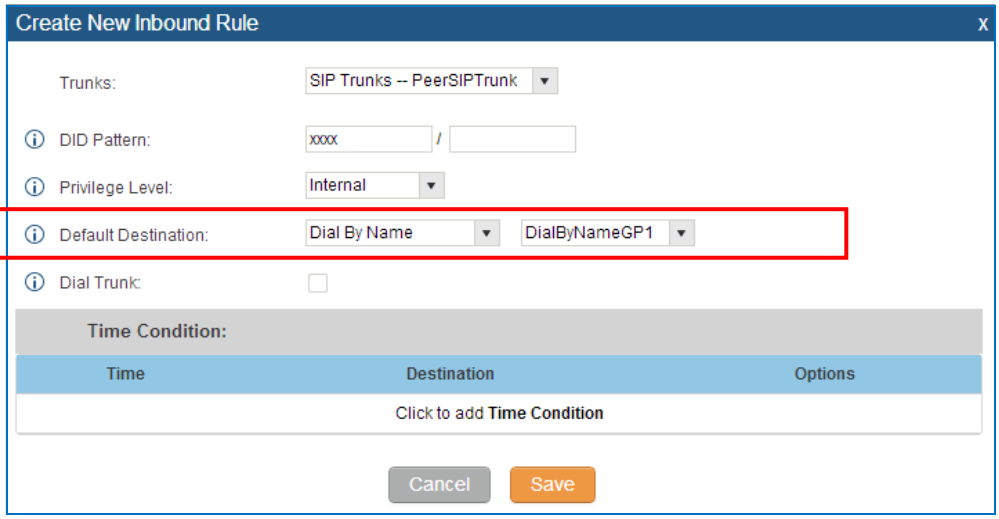


Figure 137: Dial By Name Group In Inbound Route

2. **Extension**

   Configure the direct dial extension for the Dial By Name group.

3. **Available Extensions/Selected Extensions**

   Select available extensions from the left side to the right side as the directory for the Dial By Name group. Only the selected extensions here can be reached by the Dial By Name IVR when dialing into this group. The extensions here must have valid first name and last name configured under web GUI->**PBX**->**Basic/Call Routes**->**Extensions** in order to be searchable in Dial By Name directory through IVR. By specifying the extensions here, the administrators can make sure unscreened calls will not reach the company employee if he/she doesn't want to receive them directly.

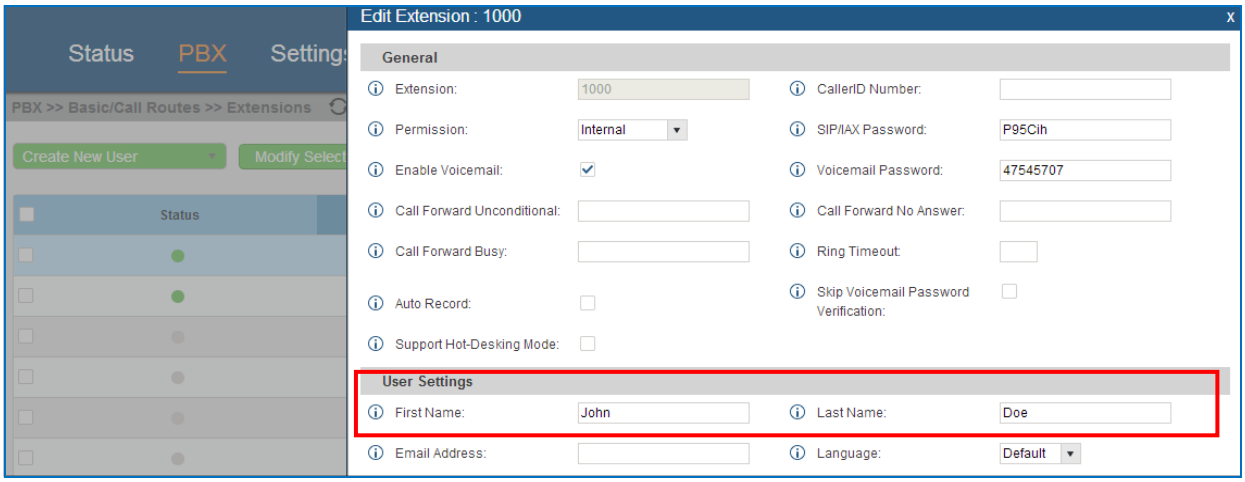


Figure 138: Configure Extension First Name and Last Name

4. **Query Type**

   Specify the query type. This defines how the caller will need to enter to search the directory.

   By First Name: enter the first 3 digits of the first name to search the directory.

   By Last Name: enter the first 3 digits of the last name to search the directory.

   By Full Name: enter the first 3 digits of the first name or last name to search the directory.

5. **Select Type**

   Specify the select type on the searching result. The IVR will confirm the name/number for the party the caller would like to reach before dialing out

   By Order: After the caller enters the digits, the IVR will announce the first matching party's name and number. The caller can confirm and dial out if it's the destination party, or press * to listen to the next matching result if it's not the desired party to call.

   By Menu: After the caller enters the digits, the IVR will announce 8 matching results. The caller can press number 1 to 8 to select and call, or press 9 for results in next page.

This page intentionally left blank

ACTIVE CALLS AND MONITOR

The active calls on the UCM6510 are displayed in web UI->**Status**->**Active Calls** page. Users can monitor call status, hang up active call(s) as well as barge in active call(s) in real time manner.

ACTIVE CALLS STATUS

To view the status of active calls, navigate to web GUI->**Status**->**Active Calls**. The following figure shows extension 1000 is calling 1001. 1001 is ringing.

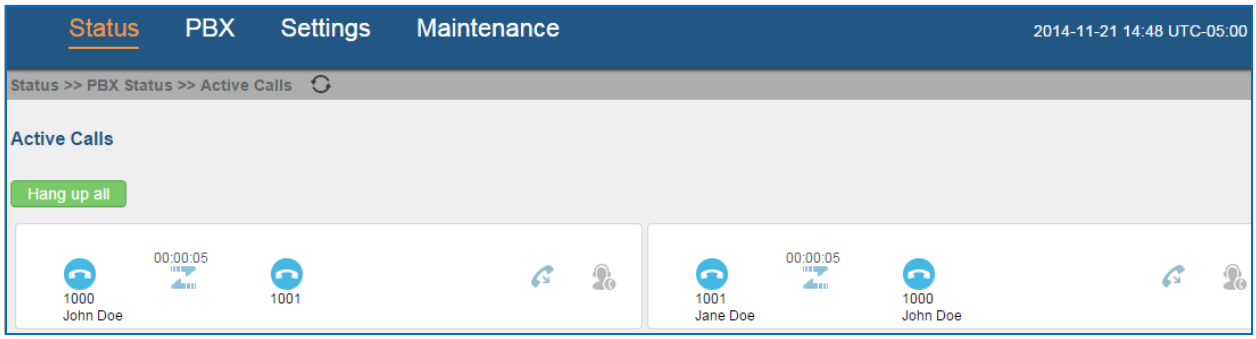


Figure 139: Status->PBX Status->Active Calls - Ringing

The following figure shows the call between 1000 and 1001 is established.

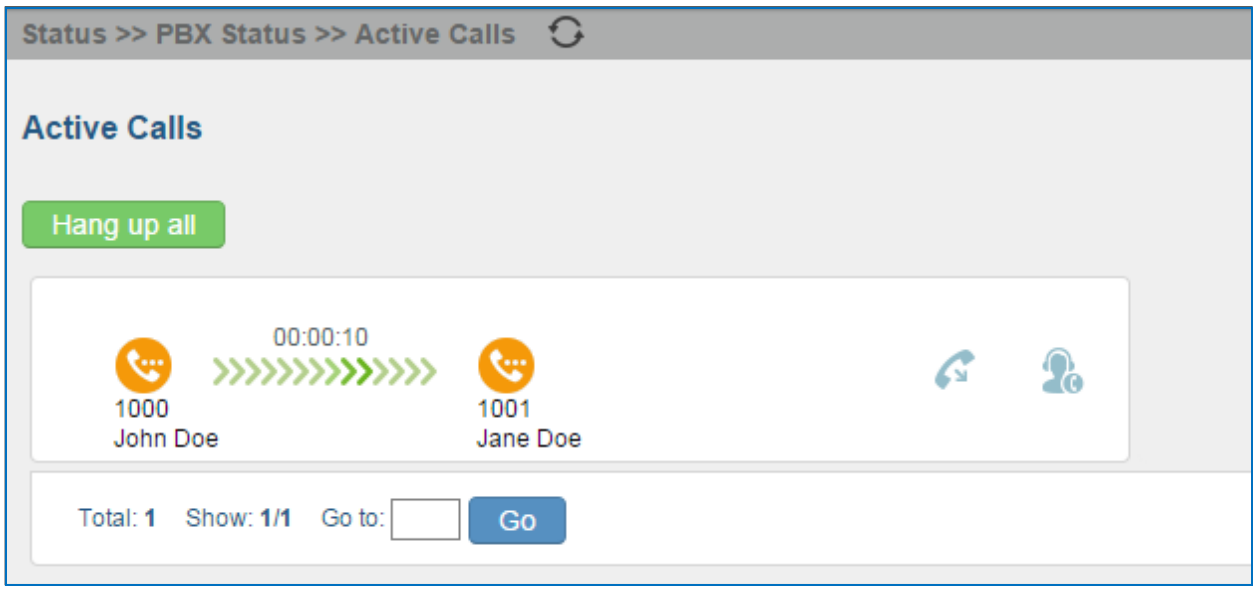


Figure 140: Status->PBX Status->Active Calls – Call Established

On Active Calls page, click on to refresh the status of active calls.

HANG UP ACTIVE CALLS

To hang up an active call, click on icon in the active call dialog. Users can also click on Hang up all to hang up all active calls shown on the Active Calls page.

CALL MONITOR

During an active call, click on icon and the Monitor dialog will pop up.

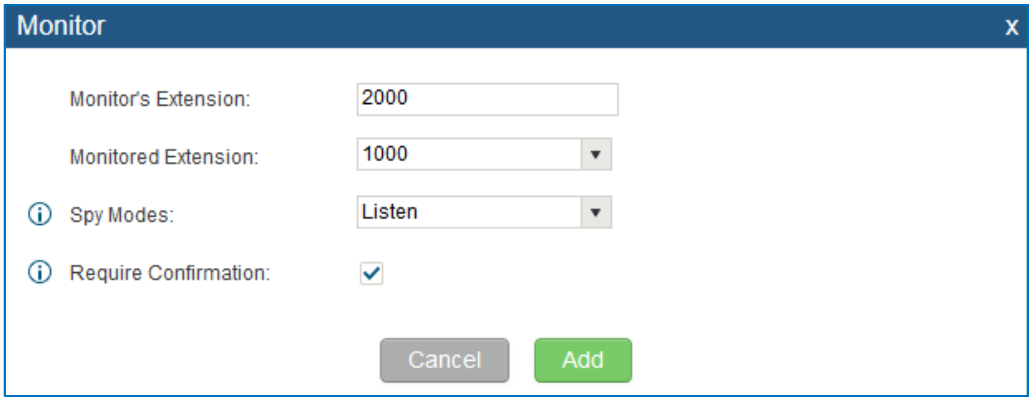


Figure 141: Configure to Monitor an Active Call

In the "Monitor" dialog, configure the following to monitor an active call:

1. Enter an available extension for "Monitor's Extension" which will be used to monitor the active call.
2. "Monitored Extension" must be one of the parties in the active call to be monitored.
3. Select spy mode. There are three options in "Spy Mode".
   - Listen
     In "Listen" mode, the extension monitoring the call can hear both parties in the active call but the audio of the user on this extension will not be heard by either party in the monitored active call.
   - Whisper
     In "Whisper" mode, the extension monitoring the call can hear both parties in the active call. The user on this extension can only talk to the selected monitored extension and he/she will not be heard by the other party in the active call. This can be usually used to supervise calls.
   - Barge
     In "Barge" mode, the extension monitoring the call can talk to both parties in the active call. The call will be established similar to three-way conference.

4. Enable or disable “Require Confirmation” option. If enabled, the confirmation of the invited monitor’s extension is required before the active call can be monitored. This option can be used to avoid adding participant who has auto-answer configured or call forwarded to voicemail.
5. Click on “Add”. An INVITE will be sent to the monitor’s extension. The monitor can answer the call and start monitoring. If “Require Confirmation” is enabled, the user will be asked to confirm to monitor the call.

Another way to monitor active calls is to dial the corresponding feature codes from an extension. Please refer to ***[Table 81: UCM6510 Feature Codes]*** and ***[ENABLE SPY]*** section for instructions.

This page intentionally left blank

CALL FEATURES

The UCM6510 supports call recording, transfer, call forward, call park and other call features via feature code**.** Feature Codes settings can be found at **web GUI->PBX->Internal Options->Feature Codes**. This section lists all the feature codes in the UCM6510 and describes how to use the call features.

FEATURE CODES

Table 81: UCM6510 Feature Codes

Feature Maps	
Blind Transfer	• Default code: #1. • Enter the code during active call. After hearing "Transfer", you will hear dial tone. Enter the number to transfer to. Then the user will be disconnected and transfer is completed. • Options **Disable** **Allow Caller**: Enable the feature code on caller side only. **Allow Callee**: Enable the feature code on callee side only. **Allow Both**: Enable the feature code on both caller and callee.
Attended Transfer	• Default code: *2. • Enter the code during active call. After hearing "Transfer", you will hear the dial tone. Enter the number to transfer to and the user will be connected to this number. Hang up the call to complete the attended transfer. • Options **Disable** **Allow Caller**: Enable the feature code on caller side only. **Allow Callee**: Enable the feature code on callee side only. **Allow Both**: Enable the feature code on both caller and callee.
Disconnect	• Default code: *0. • Enter the code during active call. It will disconnect the call. • Options **Disable** **Allow Caller**: Enable the feature code on caller side only. **Allow Callee**: Enable the feature code on callee side only. **Allow Both**: Enable the feature code on both caller and callee.
Call Park	• Default code: #72. • Enter the code during active call to park the call.

	• Options **Disable** **Allow Caller**: Enable the feature code on caller side only. **Allow Callee**: Enable the feature code on callee side only. **Allow Both**: Enable the feature code on both caller and callee.
Audio Mix Record	• Default code: *3. • Enter the code followed by # or SEND to start recording the audio call and the UCM6510 will mix the streams natively on the fly as the call is in progress. • Options **Disable** **Allow Caller**: Enable the feature code on caller side only. **Allow Callee**: Enable the feature code on callee side only. **Allow Both**: Enable the feature code on both caller and callee.
DND/Call Forward	
Do Not Disturb (DND) Activate	• Default code: *77.
Do Not Disturb (DND) Deactivate	• Default code: *78.
Call Forward Busy Activate	• Default Code: *90. • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.
Call Forward Busy Deactivate	• Default Code: *91.
Call Forward No Answer Activate	• Default Code: *92. • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.
Call Forward No Answer Deactivate	• Default Code: *93.
Call Forward Unconditional Activate	• Default Code: *72. • Enter the code and follow the voice prompt. Or enter the code followed by the extension to forward the call.
Call Forward Unconditional Deactivate	• Default Code: *73.
Feature Misc	
Feature Code Digits Timeout	• Default Setting: 1000. • Configure the maximum interval (in milliseconds) between the digits input to activate the feature code.
Call Park	• Default Extension: 700. • During an active call, initiate blind transfer and then enter this code to park the call.

Parked Lots	• Default Extension: 701-720. • These are the extensions where the calls will be parked, i.e., parking lots that the parked calls can be retrieved.
Use Parklot as Extension	If checked, the parklot number will be used as an extension and the user can transfer to the parklot number to park the call. Please note the parking lot number should not be configured the same as existing extension number. Otherwise, there will be conflict.
Parking Timeout (s)	• Default setting: 300. • This is the timeout allowed for a call to be parked. After the timeout, if the call is not picked up, the extension who parks the call will be called back.
Feature Codes	
Voicemail Access Code	• Default Code: *98. • Enter *98 and follow the voice prompt. Or dial *98 followed by the extension and # to access the entered extension's voicemail box.
My Voicemail	• Default Code: *97. • Press *97 to access the voicemail box.
Agent Pause	• Default Code: *83. • Pause the agent in all call queues.
Agent Unpause	• Default Code: *84. • Unpause the agent in all call queues.
Paging Prefix	• Default Code: *81. • To page an extension, enter the code followed by the extension number.
Intercom Prefix	• Default Code: *80. • To intercom an extension, enter the code followed by the extension number.
Blacklist Add	• Default Code: *40. • To add a number to blacklist for inbound route, dial *40 and follow the voice prompt to enter the number.
Blacklist Remove	• Default Code: *41. • To remove a number from current blacklist for inbound route, dial *41 and follow the voice prompt to remove the number.
Call Pickup on Ringing	• Default Code: **. • To pick up a call for any extension xxxx, enter the code followed by the extension number xxxx.
Pickup Extension	• Default Code: *8. • This code is for the pickup group which can be assigned for

	each extension on the extension configuration page. • If there is an incoming call to an extension, the other extensions within the same pickup group can dial *8 directly to pick up the call.
Direct Dial Voicemail Prefix	• Default Code: * • This code is for the user to directly dial or transfer to an extension's voicemail. • For example, directly dial *5000 will have to call go into the extension 5000's voicemail. If the user would like to transfer the call to the extension 5000's voicemail, enter *5000 as the transfer target number.
Call Completion Request	• Default Code: *11 • This code is for the user who wants to use Call Completion to complete a call.
Call Completion Cancel	• Default Code: *12 • This code is for the user who wants to cancel Call Completion request.
Enable Spy	• Check this box to enable spy feature codes.
Listen Spy	• This is the feature code to listen in on a call to monitor performance. Monitor's line will be muted, and neither party will hear from the monitor's extension. The default setting is *54.
Whisper Spy	• This is the feature code to speak to one side of the call (for example, whisper to employees to help them handle a call). Only one side will be able to hear from the monitor's extension. The default setting is *55.
Barge Spy	• This is the feature code to join in on the call to assist both parties. The default setting is *56.

CALL RECORDING

The UCM6510 allows users to record audio during the call. If "Auto Record" is turned on for extension or trunk, the call will be automatically recorded when there is established call with the extension or trunk. Otherwise, please follow the instructions below to manually record the call.

1. Make sure the feature code for "Audio Mix Record" is configured and enabled.
2. After establishing the call, enter the "Audio Mix Record" feature code (by default *3) followed by # or SEND to start recording.

3. To stop the recording, enter the "Audio Mix Record" feature code (by default *3) followed by # or SEND again. Or the recording will be stopped once the call hangs up.

4. The recording file can be retrieved under web GUI->**Status**->**CDR**. Click on to play the recording or click on to download the recording file.

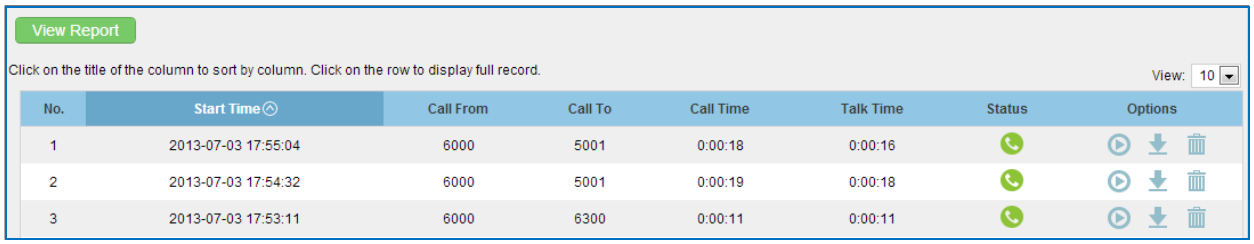

View Report
Click on the title of the column to sort by column. Click on the row to display full record.
View: 10
No. Start Time Call From Call To Call Time Talk Time Status Options
1 2013-07-03 17:55:04 6000 5001 0:00:18 0:00:16
2 2013-07-03 17:54:32 6000 5001 0:00:19 0:00:18
3 2013-07-03 17:53:11 6000 6300 0:00:11 0:00:11

Figure 142: Download Recording File from CDR Page

The above recorded call's recording files are also listed under the UCM6510 web GUI->**CDR**->**Recording Files**.

CALL PARK

The UCM6510 provides call park and call pickup features via feature code.

PARK A CALL

There are two feature codes that can be used to park the call.

- Feature Maps->Call Park (Default code #72)
  During an active call, press #72 and the call will be parked. Parking lot number (default range 701 to 720) will be announced after parking the call.

- Feature Misc->Call Park (Default code 700)
  During an active call, initiate blind transfer (default code #1) and then dial 700 to park the call. Parking lot number (default range 701 to 720) will be announced after parking the call.

RETRIEVE THE PARKED CALL

To retrieve the parked call, simply dial the parking lot number and the call will be established. If a parked call is not retrieved after the timeout, the original extension who parks the call will be called back.

ENABLE SPY

If “Enable Spy” option is enabled, feature codes for Listen Spy, Whisper Spy and Barge Spy are available for users to dial from any extension to perform the corresponding actions.

Assume a call is on-going between extension A and extension B, user could dial the feature code from extension C to listen on their call (*54 by default), whisper to one side (*55 by default), or barge into the call (*56 by default). Then the user will be asked to enter the number to call, which should be either side of the active call, extension A or B in this example.

Warning:

“Enable Spy” allows any user to listen to any call by dialing feature codes. This may result in the leakage of user privacy. Please be aware of the associated potential security risk when enabling this feature.

INTERNAL OPTIONS

This section describes internal options that haven't been mentioned in previous sections yet. The settings in this section can be applied globally to the UCM6510, including general configurations, jitter buffer, RTP settings, hardware config and STUN monitor. The options can be accessed via web GUI->**PBX**->**Internal Options**.

INTERNAL OPTIONS/GENERAL

Table 82: Internal Options/General

General Preferences	
Global OutBound CID	Configure the global CallerID used for all outbound calls when no other CallerID is defined with higher priority. If no CallerID is defined for extension or trunk, the global outbound CID will be used as CallerID.
Global OutBound CID Name	Configure the global CallerID Name used for all outbound calls. If configured, all outbound calls will have the CallerID Name set to this name. If not, the extension's CallerID Name will be used.
Operator Extension	Specify the operator extension, which will be dialed when users presses 0 to exit voicemail application. The operator extension can also be used in IVR option.
Ring Timeout	Configure the number of seconds to ring an extension before the call goes to the user's voicemail box. The default setting is 60. **Note:** This is the global value used for each extension if "Ring Timeout" field is left empty on the extension configuration page.
Record Prompt	If enabled, users will hear voice prompt before recording is started or stopped. For example, before recording, the UCM6510 will play voice prompt "The call will be recorded". The default setting is "No".
Extension Preferences	
Enforce Strong Passwords	If enabled, strong password will be enforced for the password created on the UCM6510. The default setting is enabled. Strong Password Rules: 1. Password for voicemail, voicemail group, outbound route, DISA, call queue and conference requires non-repetitive and non-sequential digits, with a minimum length of 4 digits. Repetitive digits pattern (such

	as 0000, 1111, 1234, 2345, and etc), or common digits pattern (such as 111222, 321321 and etc) are not allowed to be configured as password. 2. Password for extension registration, web GUI admin login, LDAP and LDAP sync requires alphanumeric characters containing at least two categories of the following, with a minimum length of 4 characters. ・ Numeric digits ・ Lowercase alphabet characters ・ Uppercase alphabet characters ・ Special characters
Enable Random Password	If enabled, random password will be generated when the extension is created. The default setting is "Yes". It is recommended to enable it for security purpose.
Disable Extension Range	If set to "Yes", users could disable the extension range pre-configured/configured on the UCM6510. The default setting is "No". The default extension range assignment is shown in “Extension Ranges” below. **Note:** It is recommended to keep the system assignment to avoid inappropriate usage and unnecessary issues.
Extension Ranges	The default extension range assignment is: • User Extensions: 1000-6299 User Extensions is referring to the extensions created under web UI->**PBX**->**Basic/Call Routes**->**Extensions** page. • Pick Extensions: 4000-4999 This refers to the extensions that can be manually picked from end device when being provisioned by the UCM6510. There are two related options in zero config page->Auto Provision Settings, "Pick Extension Segment" and "Enable Pick Extension". If "Enable Pick Extension" under zero config settings is selected, the extension list defined in "Pick Extension Segment" will be sent out to the device after receiving the device's request. This "Pick Extension Segment" should be a subset of the "Pick Extensions" range here. This feature is for the GXP series phones that support selecting extension to be provisioned via phone's LCD.

	• Auto Provision Extensions: 5000-6299 This sets the range for "Zero Config Extension Segment" which is the extensions can be assigned on the UCM6510 to provision the end device. • Conference Extensions: 6300-6399 • Ring Group Extensions: 6400-6499 • Queue Extensions: 6500-6599 • Voicemail Group Extensions: 6600-6699 • IVR Extensions: 7000-7100 • Fax Extensions: 7200-8200

INTERNAL OPTIONS/JITTER BUFFER

Table 83: Internal Options/Jitter Buffer

SIP Jitter Buffer	
Enable Jitter Buffer	Select to enable jitter buffer on the sending side of the SIP channel. The default setting is "No".
Jitter Buffer Size	Configure the time (in ms) to buffer. This is the jitter buffer size used in "Fixed" jitter buffer, or used as the initial time for "adaptive" jitter buffer. The default setting is 100.
Max Jitter Buffer	Configure the maximum time (in ms) to buffer for "Adaptive" jitter buffer implementation, or used as the jitter buffer size for "Fixed" jitter buffer implementation. The default setting is 200.
Implementation	Configure the jitter buffer implementation on the sending side of a SIP channel. The default setting is "Fixed". • **Fixed** The size is always equal to the value of "Max Jitter Buffer". • **Adaptive** The size is adjusted automatically and the maximum value equals to the value of "Max Jitter Buffer".

INTERNAL OPTIONS/RTP SETTINGS

Table 84: Internal Options/RTP Settings

RTP Start	Configure the RTP port starting number. The default setting is 10000.

RTP End	Configure the RTP port ending address. The default setting is 20000.
Strict RTP	Configure to enable or disable strict RTP protection. If enabled, RTP packets that do not come from the source of the RTP stream will be dropped. The default setting is "Disable".
RTP Checksums	Configure to enable or disable RTP Checksums on RTP traffic. The default setting is "Disable".

INTERNAL OPTIONS/STUN MONITOR

Table 85: Internal Options/STUN Monitor

STUN Server	Configures the IP address or URL of the STUN server to query. If not specified, STUN is disabled. The default setting is stun.ipvideotalk.com. Valid format: [(hostname | IP-address) [':' port] The default port number is 3478 if not specified.
STUN Refresh	Configure the number of seconds between STUN Refreshes. The default setting is 30 seconds.

IAX SETTINGS

The UCM6510 IAX global settings can be accessed via web GUI->**PBX**->**IAX Settings**.

IAX SETTINGS/GENERAL

Table 86: IAX Settings/General

Bind Port	Configure the port number that the IAX2 will be allowed to listen to. The default setting is 4569.
Bind Address	Configure the address that the IAX2 will be forced to bind to. The default setting is 0.0.0.0, which means all addresses.
IAX1 Compatibility	Select to configure IAX1 compatibility. The default setting is "No".
No Checksums	If selected, UDP checksums will be disabled and no checksums will be calculated/checked on systems supporting this features. The default setting is "No".
Delay Reject	If enabled, the IAX2 will delay the rejection of calls to avoid DOS. The default setting is "No".
ADSI	Select to enable ADSI phone compatibility. The default setting is "No".
Music On Hold Interpret	Specify which Music On Hold class this channel would like to listen to when being put on hold. This music class is only effective if this channel has no music class configured and the bridged channel putting the call on hold has no "Music On Hold Suggest" setting.
Music On Hold Suggest	Specify which Music On Hold class to suggest to the bridged channel when putting the call on hold.
Bandwidth	Configure the bandwidth for IAX settings. The default setting is "Low".

IAX SETTINGS/REGISTRATION

Table 87: IAX Settings/Registration

IAX Registration Options	
Min Reg Expire	Configure the minimum period (in seconds) of registration. The default setting is 60.
Max Reg Expire	Configure the maximum period (in seconds) of registration. The default setting is 3600.
IAX Thread Count	Configure the number of IAX helper threads. The default setting is 10.
IAX Max Thread Count	Configure the maximum number of IAX threads allowed. The default setting is 100.

Auto Kill	If set to "yes", the connection will be terminated if ACK for the NEW message is not received within 2000ms. Users could also specify number (in milliseconds) in addition to "yes" and "no". The default setting is "yes".
Authentication Debugging	If enabled, authentication traffic in debugging will not show. The default setting is "No".
Codec Priority	Configure codec negotiation priority. The default setting is "Reqonly". • Caller Consider the callers preferred order ahead of the host's. • Host Consider the host's preferred order ahead of the caller's. • Disabled Disable the consideration of codec preference all together. • Reqonly This is almost the same as "Disabled", except when the requested format is not available. The call will only be accepted if the requested format is available.
Type of Service	Configure ToS bit for preferred IP routing.
IAX Trunk Options	
Trunk Frequency	Configure the frequency of trunk frames (in milliseconds). The default setting is 20.
Trunk Time Stamps	If enabled, time stamps will be attached to trunk frames. The default setting is "No".

IAX SETTINGS/STATIC DEFENSE

Table 88: IAX Settings/Static Defense

Call Token Optional	Enter a single IP address or a range of IP addresses for which call token validation is not required. For example: 11.11.11.11 11.11.11.11/22.22.22.22.
Max Call Numbers	Configure the maximum number of calls allowed for a single IP address.
Max Unvalidated Call Numbers	Configure the maximum number of unvalidated calls for all IP addresses.
Call Number Limits	Configure to limit the number of calls for a give IP address of IP range.
IP or IP Range	Enter the IP address or a range of IP addresses to be considered for call number limits. For example: 11.11.11.11 11.11.11.11/22.22.22.22.

SIP SETTINGS

The UCM6510 SIP global settings can be accessed via web GUI->**PBX**->**SIP Settings**.

SIP SETTINGS/GENERAL

Table 89: SIP Settings/General

Realm For Digest Authentication	Configure the host name or domain name for the UCM6510. Realms MUST be globally unique according to RFC3261. The default setting is grandstream.
Bind UDP Port	Configure the UDP port used for SIP. The default setting is 5060.
Bind IP Address	Configure the IP address to bind to. The default setting is 0.0.0.0, which means binding to all addresses.
Allow Guest Calls	If enabled, the UCM6510 allows unauthorized INVITE coming into the PBX and the call can be made. The default setting is "No". **Warning:** Please be aware of the potential security risk when enabling "Allow Guest Calls" as this will allow any user with the UCM6510 address to dial into the UCM6510.
Overlap Dialing	Select to enable overlap dialing support. Overlap dial provides for a longer time-out period between digits, also called the inter-digit timer. If set to "Yes", the PBX expects to receive the digits one right after the other coming in to this line with very little delay between digits. If set to "No", the PBX waits up to about 2 seconds between digits. The default setting is "No".
Allow Transfer	If set to "No", all transfers initiated by the endpoint in the UCM6510 will be disabled (unless enabled in peers or users). The default setting is "Yes".
Enable DNS SRV Lookups on Outbound Calls	Select to enables DNS SRV lookups on outbound calls from the UCM6510. The default setting is "Yes".
MWI From	When sending MWI NOTIFY requests, this value will be used in the "From:" header as the "name" field. If no "From User" is configured, the "user" field of the URI in the "From:" header will be filled with this value.
SIP Domain Support	
Domain	Configure the domain for the UCM6510. Incoming INVITE and REFER messages can be matched against a list of "allowed" domains, each of which can direct the call to a specific context if desired. By default, all

	domains are accepted and sent to the default context or the context associated with the user/peer placing the call. Register to non-local domains will be automatically denied if a domain list is configured. Up to 10 domains can be added.
From Domain	Configure the domain in the "From:" header of the SIP message. It may be required by some providers for authentication.
Auto Domain	If enabled, the UCM6510 will add local host name and local IP to domain list. The default setting is "No".
Allow External Domains	If enabled, requests for external domains that are not served by the UCM6510 will be allowed. The default setting is "Yes".

SIP SETTINGS/MISC

Table 90: SIP Settings/Misc

Outbound SIP Registrations	
Register Timeout	Configure the register retry timeout (in seconds). The default setting is 20.
Register Attempts	Configure the number of registration attempts before the UCM6510 gives up. The default setting is 0, which means the UCM6510 will keep trying until the server side accepts the registration request.
Video	
Max Bit Rate (kb/s)	Configure the maximum bit rate (in kb/s) for video calls. The default setting is 384.
Support SIP Video	Select to enable video support in SIP calls. The default setting is "Yes".
Generate Manager Events	If enabled, the UCM6510 will generate manager events when SIP UA performs events (e.g. Hold). The default setting is "No".
Reject Non-Matching INVITE	If enabled, when rejecting an incoming INVITE or REGISTER request, the UCM6510 will always reject with "401 Unauthorized" instead of notifying the requester whether there is a matching user or peer for the request. This reduces the ability of an attacker to scan for valid SIP usernames. The default setting is "No".

SIP SETTINGS/SESSION TIMER

Table 91: SIP Settings/Session Timer

Session Timers	Select the session timer mode. The default setting is "Accept". The options are: • Originate Always request and run session timer. • Accept

	Run session timer only when requested by other UA. • Refuse Do not run session timer.
Session Expire	Configure the maximum session refresh interval (in seconds). The default setting is 1800.
Min SE	Configure the minimum session refresh interval (in seconds). The default setting is 90.
Session Refresher	Select the session refresher to be UAC or UAS. The default setting is UAC.

SIP SETTINGS/TCP and TLS

⚠ **Note:**

The configuration in this section requires system reboot to take effect.

Table 92: SIP Settings/TCP and TLS

TCP Enable	Configure to allow incoming TCP connections with the UCM6510. The default setting is "No".
TCP Bind Address	Configure the IP address for TCP server to bind to. 0.0.0.0 means binding to all interfaces. The port number is optional. If not specified, 5060 will be used.
TLS Enable	Configure to allow incoming TLS connections with the UCM6510. The default setting is "No".
TLS Bind Address	Configure the IP address for TLS server to bind to. 0.0.0.0 means binding to all interfaces. The port number is optional. If not specified, 5061 will be used. **Note:** The IP address must match the common name (hostname) in the certificate. Please do not bind a TLS socket to multiple IP addresses. For details on how to construct a certificate for SIP, please refer to the following document: http://tools.ietf.org/html/draft-ietf-sip-domain-certs
TLS Client Protocol	Select the TLS protocol for outbound client connections. The default setting is TLSv1.
TLS Do Not Verify	If enabled, the TLS server's certificate won't be verified when acting as a

	client. The default setting is "Yes".
TLS Self-Signed CA	This is the CA certificate if the TLS server being connected to requires self-signed certificate, including server's public key. This file will be renames as "TLS.ca" automatically. **Note:** The size of the uploaded ca file must be under 2MB.
TLS Cert	This is the Certificate file (*.pem format only) used for TLS connections. It contains private key for client and signed certificate for the server. This file will be renamed as "TLS.pem" automatically. **Note:** The size of the uploaded certificate file must be under 2MB.
TLS CA Cert	This file must be named with the CA subject name hash value. It contains CA's (Certificate Authority) public key, which is used to verify the accessed servers. **Note:** The size of the uploaded CA certificate file must be under 2MB.
TLS CA List	Display a list of files under the CA Cert directory.

SIP SETTINGS/NAT

Table 93: SIP Settings/NAT

External IP Address	Configure a static address and port (optional) that will be used in outbound SIP messages if the UCM6510 is behind NAT. If it's a hostname, it will only be looked up once.
External Host	Specify an external host name, which is similar to External Address except the host name will be looked up periodically based on the "External Refresh" interval.
External Refresh	Configure the refresh interval for the external host (if used) The default setting is 10.
External TCP Port	Configure the externally mapped TCP port when the UCM6510 is behind a static NAT or PAT.
External TLS Port	Configures the externally mapped TLS port when UCM6510 is behind a static NAT or PAT.
Local Network Address	Specify a list of network addresses that are considered inside of the NAT network. Multiple entries are allowed. If not configured, the external IP address will not be set correctly.

	A sample configuration could be as follows: 192.168.0.0/16

SIP SETTINGS/TOS

Table 94: SIP Settings/ToS

ToS For SIP	Configure the Type of Service for SIP packets. The default setting is None.
ToS For RTP Audio	Configure the Type of Service for RTP audio packets. The default setting is None.
ToS For RTP Video	Configure the Type of Service for RTP video packets. The default setting is None.
Default Incoming/Outgoing Registration Time	Configure the default duration (in seconds) of incoming/outgoing registration. The default setting is 120.
Max Registration/Subscription Time	Configure the maximum duration (in seconds) of incoming registration and subscription allowed by the UCM6510. The default setting is 3600.
Min Registration/Subscription Time	Configure the minimum duration (in seconds) of incoming registration and subscription allowed by the UCM6510. The default setting is 60.
Music On Hold Interpret	Configure the Music On Hold class for the channel when being put on hold. This is used when the Music On Hold class is not set on the channel and the peer channel placing the call on hold doesn't have "Music On Hold Suggest".
Music On Hold Suggest	Configure the Music On Hold class to suggest to the peer channel when placing the peer on hold.
Enable Relaxed DTMF	Select to enable relaxed DTMF handling. The default setting is "No".
DTMF Mode	Select DTMF mode to send DTMF. The default setting is RFC2833. If "Info" is selected, SIP INFO message will be used. If "Inband" is selected, 64-kbit codec PCMU and PCMA are required. When "Auto" is selected, "RFC2833" will be used if offered, otherwise "Inband" will be used. The default setting is "RFC2833".
RTP Timeout	During an active call, if there is no RTP activity within the timeout (in seconds), the call will be terminated. The default setting is no timeout. **Note:** This setting doesn't apply to calls on hold.
RTP Hold Timeout	When the call is on hold, if there is no RTP activity within the timeout (in seconds), the call will be terminated. This value of RTP Hold Timeout should be larger than RTP Timeout. The default setting is no timeout.
Trust Remote Party ID	Configure whether the Remote-Party-ID should be trusted. The default

	setting is "No".
Send Remote Party ID	Configure whether the Remote-Party-ID should be sent or not. The default setting is "No".
Generate In-Band Ringing	Configure whether the UCM6510 should generate inband ringing or not. The default setting is "Never". • Yes: The UCM6510 will send 180 Ringing followed by 183 Session Progress and in-band audio. • No: The UCM6510 will send 180 Ringing if 183 Session Progress has not been sent yet. If audio path is established already with 183 then send in-band ringing. • Never: Whenever ringing occurs, the UCM6510 will send 180 Ringing as long as 200OK has not been set yet. Inband ringing will not be generated even the end point device is not working properly.
Server User Agent	Configure the user agent string for the UCM6510.
Send Compact SIP Headers	If enabled, compact SIP headers will be sent. The default setting is "No".
Add "user=phone" to URI	If enabled, "user=phone" will be added to URI that contains a valid phone number. The default setting is "No".

VALUE-ADDED FEATURES

FAX SENDING

The UCM6510 supports sending Fax via web UI access. This feature can be found on web UI->**PBX**->**Value-added Features**->**Fax Sending** page. In order to send fax, pre-setup for analog trunk and outbound route is required.

After making sure analog trunk or VoIP Trunk is setup properly and UCM6510 can reach out to PSTN numbers via the trunk, on Fax Sending page, enter the fax number and upload the file to be faxed. Then click on “Send” to start. The progress of sending fax will be displayed in web UI. Users can also view the sending history is in the same web page.

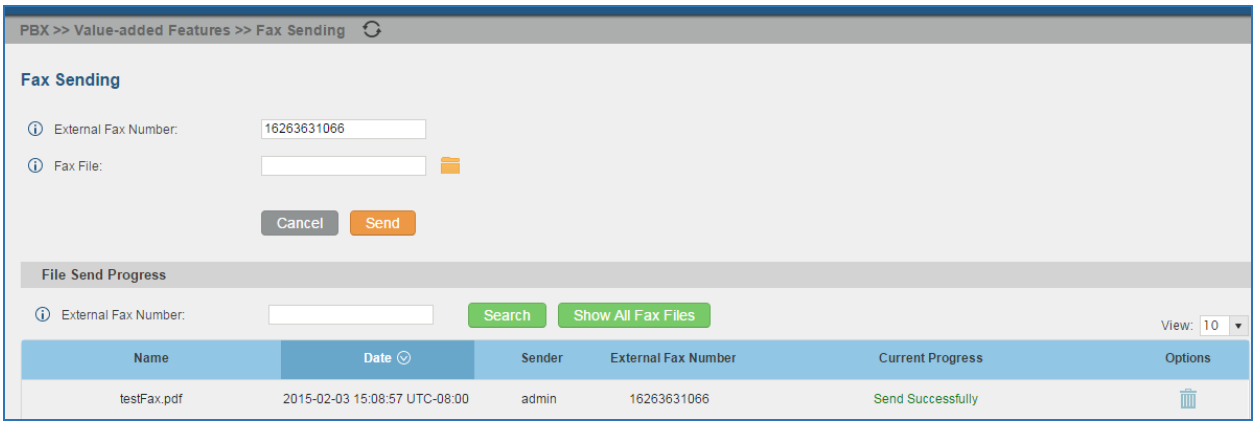


Figure 143: Fax Sending in Web UI

ANNOUNCEMENTS CENTER

UCM6510 supports Announcements Center feature starting from firmware version 1.0.2.7. Announcements Center allows users to previously record and store voice message into UCM6510 with a specified code. The users can also create group with specified extensions. When the code and the group number are dialed together in the combination of **code + group number**, the specified voice message is sent to all group members and only extensions in the group will hear the voice message.

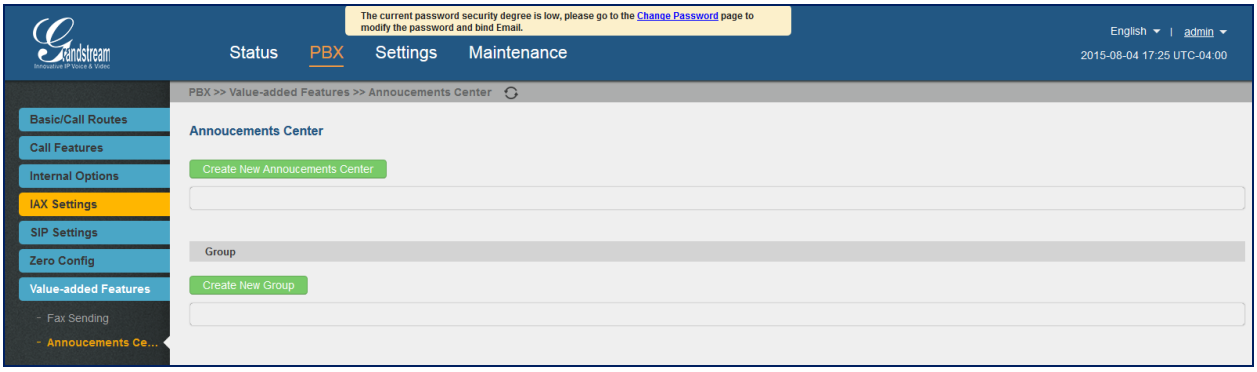


Figure 144: Announcements Center

ANNOUNCEMENTS CENTER SETTINGS

Table 95: Announcements Center Settings

Name	Configure a name for the newly created Announcements Center for identify this announcement center.
Code	Enter a code number for the custom prompt. This code will be used in combination with the group number. For example, if the code is 55, and group number is 666. The user can dial 55666 to send prompt 55 to all members in group 666. **Note:** The combination number must not conflict with any number in the system such as extension number or conference number.
Custom Prompt	This option is to set a custom prompt as an announcement to notify group members. The file can be uploaded from page 'Custom Prompt'. Click 'Prompt' to add additional record.
Ring Timeout	Configure the ring timeout for the group members. The default value is 30 seconds.

GROUP SETTINGS

Table 96: Group Settings

Name	Configure a name for the newly created group to identify the group.
Number	Configure the group number. The group number is used in combination with the code. For example, if group number is 666, and code is 55. The user can dial 55666 to send prompt 55 to all members in group 666. **Note:**

	The combination number must not conflict with any number in the system such as extension number or conference number.

Announcements Center feature can be found under web **UI-> PBX->Value-added Features-> Announcements Center**. The following example demonstrates the usage of this feature.

1. Click Create New Group to create new group.
2. Give a name to the newly created group.
3. Create a group number which is used with code to send voice message.
4. Select the extensions to be included in the group, who will receive the voice message.

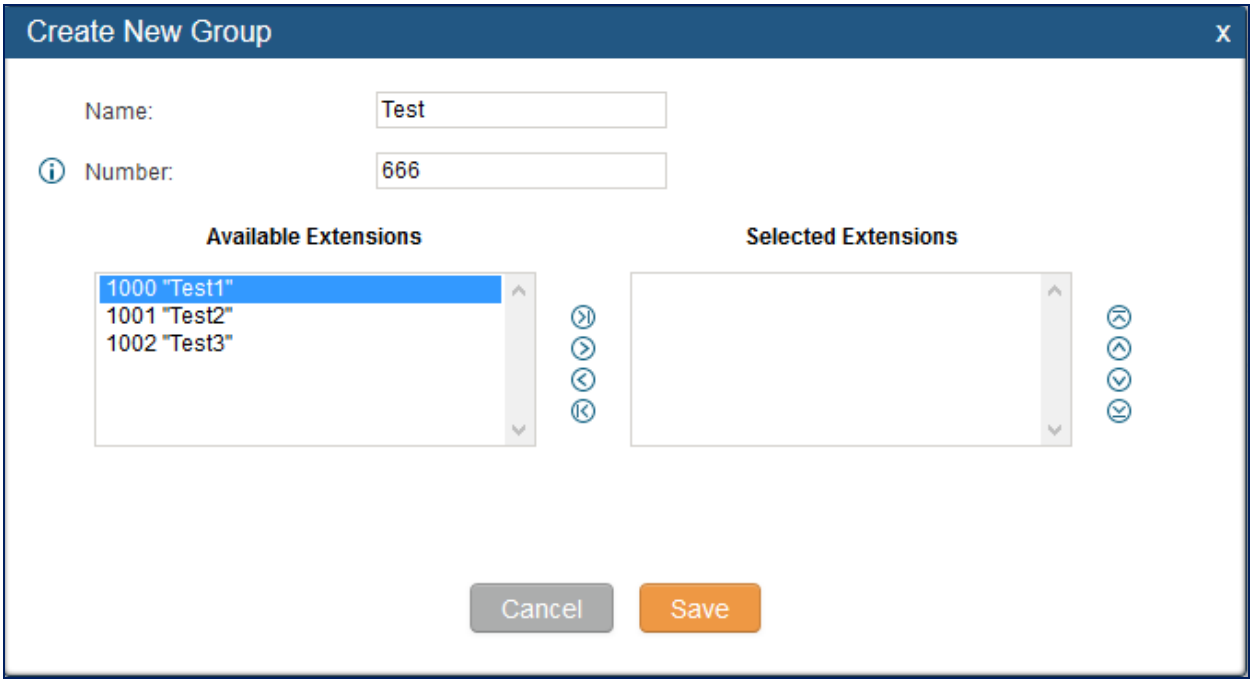


Figure 145: Announcements Center Group Configuration

In this example, group “Test” has number 666. Extension 1000, 1001 and 1002 are in this group.

5. Click Create New Annoucements Center to create a new Announcement Center.
6. Give a name to the newly created Announcement Center.
7. Specify the code which will be used with group number to send the voice message to.
8. Select the message that will be used by the code from the Custom Prompt drop down menu. To create a new Prompt, please click “Prompt” link and follow the instructions in that page.

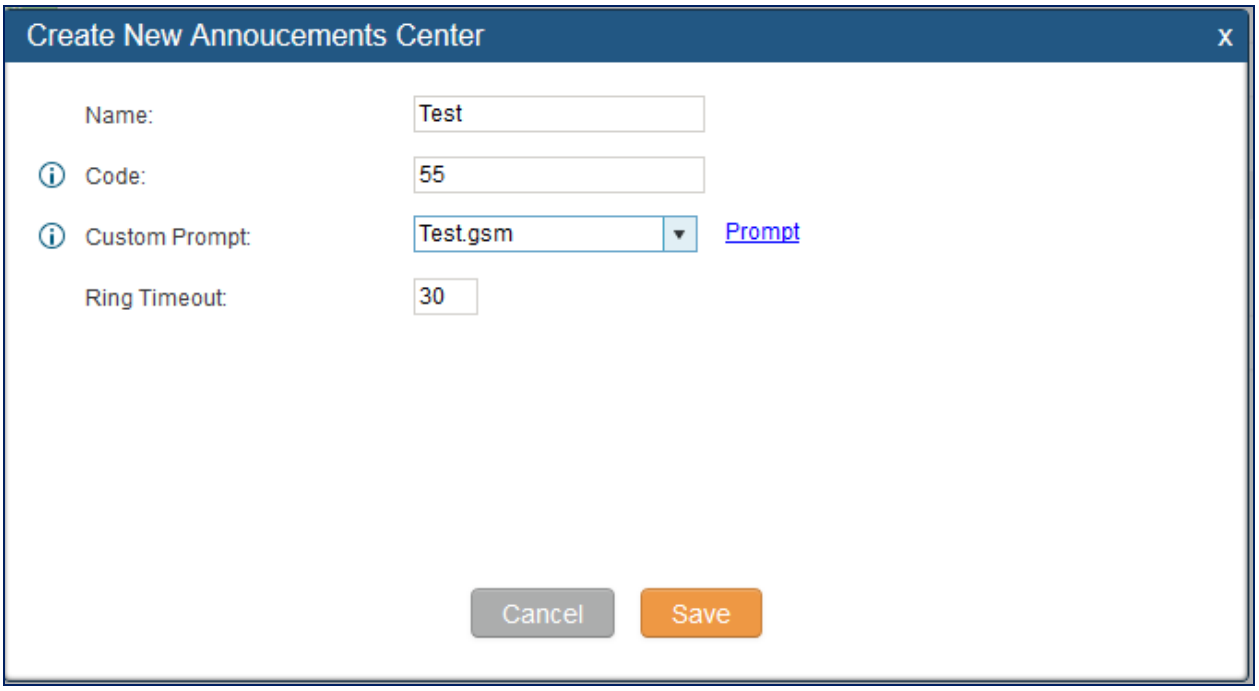


Figure 146: Announcements Center Code Configuration

Code and Group number are used together to direct specified message to the target group. All extensions in the group will receive the message. For example, we can send code 55 to group 666 by dialing 55666 from any extension registered to the UCM6100. All the members in group 666 which are extension 1000, 1001 and 1002 will receive this voice message after they pick up the call.

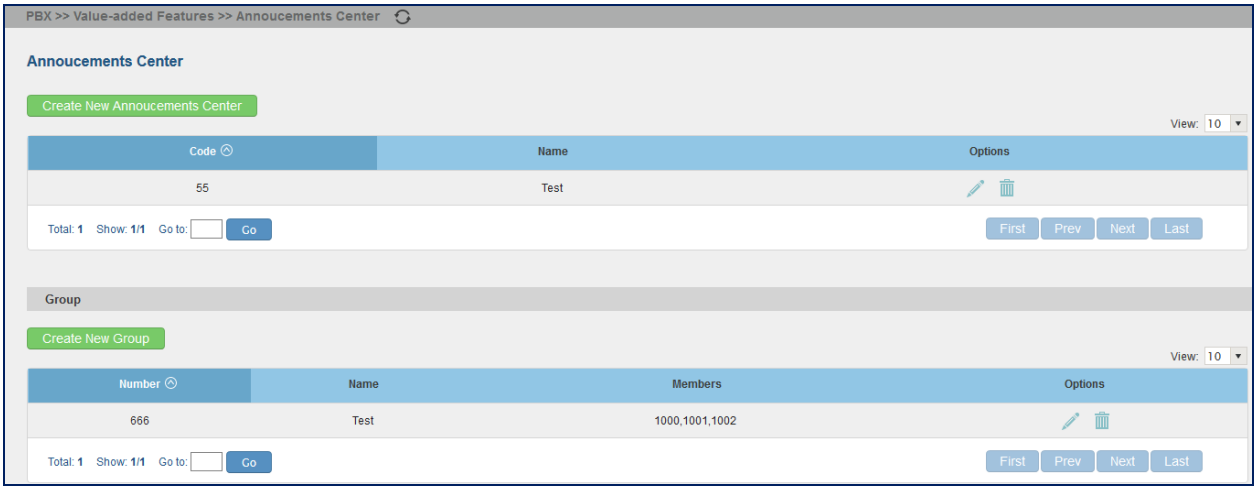


Figure 147: Announcements Center example

STATUS AND REPORTING

PBX STATUS

The UCM6510 monitors the status for Trunks, Extensions, Queues, Conference Rooms, Interfaces, Digital Channels and Parking lot. It presents administrators the real time status in different sections under web GUI->**Status**->**PBX Status**.

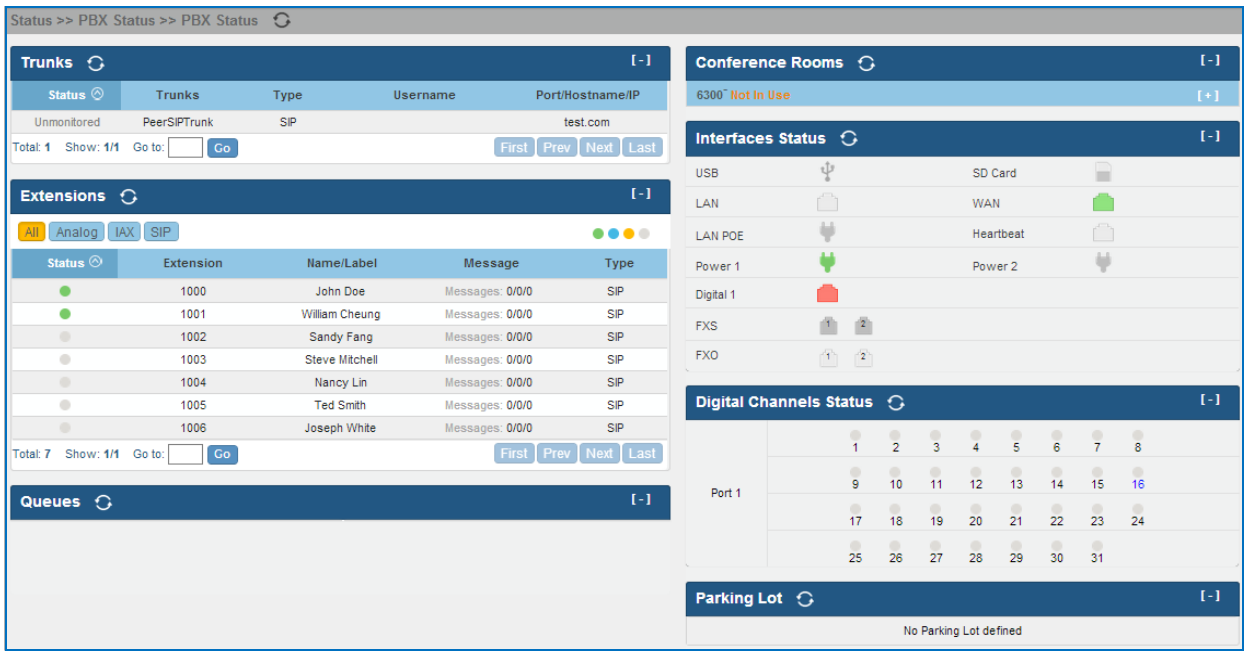


Figure 148: Status->PBX Status

TRUNKS

Users could see all the configured trunk status in this section.

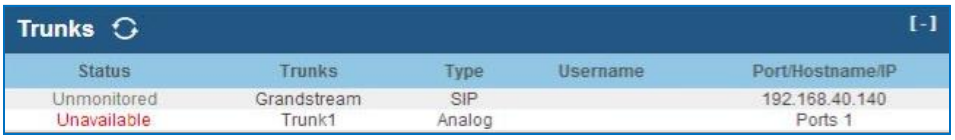


Figure 149: Trunk Status

Table 97: Trunk Status

Status	Display trunk status. • Analog trunk/Digital trunk status:

	Available **Busy** **Unavailable** **Unknown Error** **Error Configured**: Incorrect signaling configuration between the two devices. For example, both of the devices are configured as CPE or NET. • SIP Peer trunk status: **Unreachable**: The hostname cannot be reached. **Unmonitored**: QUALIFY feature is not turned on to be monitored. **Reachable**: The hostname can be reached. • SIP Register trunk status: **Registered** **Unrecognized Trunk**
Trunks	Display trunk name
Type	Display trunk Type: • Analog • E1/T1/J1 • SIP • IAX
Username	Display username for this trunk.
Port/Hostname/IP	Display Port for analog trunk, or Hostname/IP for VoIP (SIP/IAX) trunk.

Other operations are also available in trunk status section:

- Click on "Trunks", the web page will redirect to trunk configuration page which can also be accessed via web GUI->**PBX**->**Basic/Call Routes**->**Analog Trunks**.
- Click on to refresh the trunk status.
- Click on [+] to expand the status detail table.
- Click on [-] to hide the status detail table.

EXTENSIONS

Users could see all the configured extension status in this section.

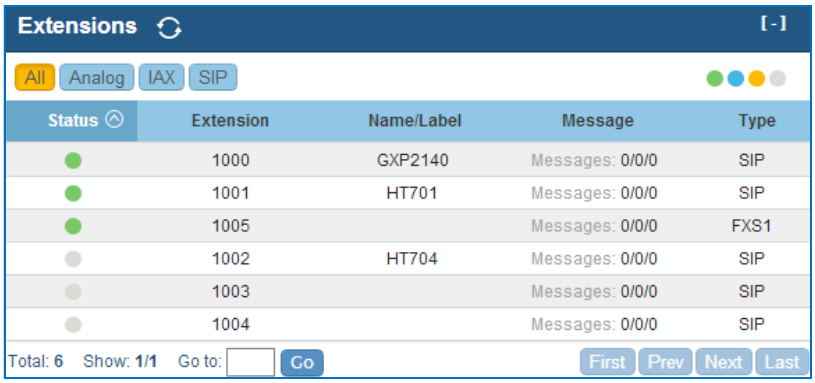


Figure 150: Extension Status

Table 98: Extension Status

Status	Display extension number (including feature code). The color indicator has the following definitions. • Green: Free • Blue: Ringing • Yellow: In Use • Grey: Unavailable
Extension	Display the extension number.
Name/Label	Display name (callerID name) or label for the extension.
Message	Display message status for the extension. Example: 2/4/1 Description: There are 2 urgent messages, 4 messages in total and 1 message that has been already read.
Type	Displays extension type. • SIP User • IAX User • Analog User (FXS) • Features

Other operations are also available in extension status section:

- Click on "Extensions", the web page will redirect to extension configuration page which can also be accessed via web GUI->**PBX**->**Basic/Call Routes**->**Extensions**.
- Click on to refresh the extension status.
- Click on one of the tabs All Analog Features IAX SIP to display the corresponding extensions accordingly.
- Click on [+] to expand the status detail table.

- Click on [-] to hide the status detail table.

QUEUES

Users could see all the configured call queue status in this section. The following figure shows the call queue 6500 being in used.

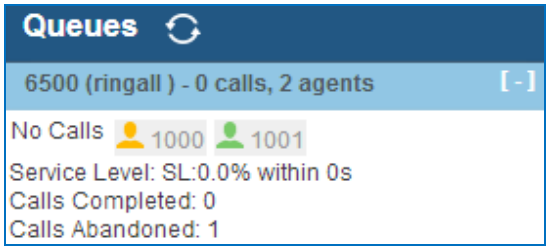


Figure 151: Queue Status

The current call status (caller ID, duration), agent status, service level, calls summary (completed/abandoned) are shown for the call queue. The agent status is defined as below.

Table 99: Agent Status

	The agent is available/idle.
	The agent is ringing.
	The agent is talking/busy.
	The agent has been logged out.

On the UCM6510, **Service Level** is defined as the percentage of high-quality calls over all calls in the call queue, where high-quality call means calls answered within 10 seconds.

Other operations are also available in queue status section:

- Click on "Queues", the web page will redirect to call queue configuration page which can also be accessed via web GUI->**PBX**->**Call Features**->**Call Queue**.
- Click on to refresh the call queue status.
- Click on [+] to expand the call queue detail.
- Click on [-] to hide the call queue detail.

CONFERENCE ROOMS

Users could see all the conference room status in this section. It shows all the configured conference rooms, current users, call duration for each user and conference call.

Figure 152: Conference Room Status

Other operations are also available in conference room status section:

- Click on "Conference Rooms", the web page will redirect to conference room configuration page which can also be accessed via web GUI->**PBX**->**Call Features**->**Conference**.
- Click on to refresh the conference room status.
- Click on [+] to expand the conference room details.
- Click on [-] to hide the conference room details.

INTERFACES STATUS

This section displays interface connection status on the UCM6510 for USB, SD Card, LAN, WAN, LAN PoE, Heartbeat, Power 1, Power 2, Digital, FXS and FXO ports.

Table 100: Interface Status Indicators

FXO	
	Disconnected
	Connected but not configured
	Connected and idle
	Connected and in use
FXS	
	Connected but not configured

	Connected and idle
	Connected and in use
SD Card	
	SD Card plugged in
	SD Card unplugged
USB	
	USB plugged in
	USB unplugged
LAN PoE	
	PoE is used
	PoE is not used
Power 1/2	
	Power supply is working
	Power supply is abnormal
	No power supply
LAN/WAN/Heart Beat	
	Connected
	Not connected
Digital Port T1/E1/J1	
	Connected and working

	RED alarm: there is physical wiring problem, loss of connectivity, or a framing/line-coding mismatch with the remote switch.
	YELLOW alarm: connected but the link is working only one-way. This means that the remote switch is not able to maintain sync with you, or is not receiving your transmission. The following example scenarios could trigger YELLOW alarm: 1. The T1 port is connected with J1 connection. 2. Incorrect cable is used. 3. When using E1, one end is using CRC4 while the other end is not.
	BLUE alarm: the port goes into BLUE alarm when it receives all unframed 1s on all timeslots from the remote switch. This is a special signal to indicate that the remote switch is having problem with its upstream connection.
	Cannot start up

Other operations are also available in interface status section:

- Click on to refresh the interface status.
- Click on [+] to expand the interface details.
- Click on [-] to hide the interface details.

DIGITAL CHANNELS STATUS

This section displays the status of the digital trunks on the UCM6510.

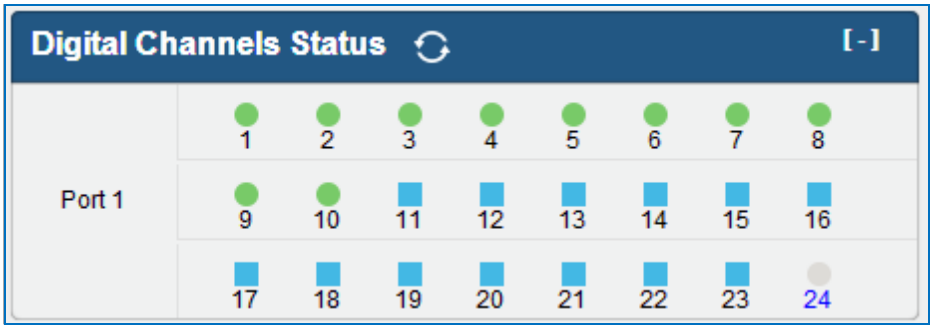


Figure 153: Digital Channels Status

Table 101: Digital Channel Status Indicators

Voice Channel	
	Not available
	Connected and in talking status; or incorrect configuration
	Connected and in idle status
	Connected and in ringing status
Data Channel	
	Always shows blue square
D Channel	
	Always shows grey with channel number in blue.

Other operations are also available in interface status section:

- Click on to refresh the Digital Channels status.
- Click on [+] to expand the Digital Channels Status details.
- Click on [-] to hide the Digital Channels Status details.

PARKING LOT

The UCM6510 supports call park using feature code. When there is call being parked, this section will display the parking lot status.

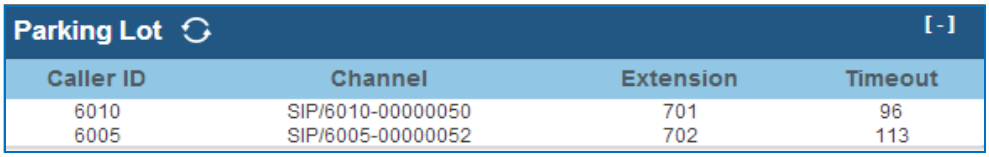


Figure 154: Parking Lot Status

Table 102: Parking Lot Status

Caller ID	Display the caller ID who parks the call.
Channel	Display channel for the call park.
Extension	Display the parking lot number where the call is parked/retrieved.
Timeout	Display timeout (in seconds) for the parked call. The status page will dynamically update this timer from 120 seconds (default) to 0. When the timer reaches 0, the caller who parks the call will be called back.

Other operations are also available in parking lot status section:

- Click on "Parking Lot", the web page will redirect to feature codes page which can also be accessed via web GUI->**PBX**->**Internal Options**->**Feature Codes**.
- Click on to refresh the parking lot status.
- Click on [+] to expand the parking lot details.
- Click on [-] to hide the parking details.

SYSTEM STATUS

The UCM6510 system status can be accessed via web GUI->**Status**->**System Status**, which displays the following system information.

- **General**
- **Network**
- **Storage Usage**
- **Resource Usage**

GENERAL

Under web GUI->**Status**->**System Status**->**General**, users could check the hardware and software information for the UCM6510. Please see details in the following table.

Table 103: System Status->General

Status ->System Status -> General	
Model	Product model.
Part Number	Product part number.
System Time	Current system time. The current system time is also available on the upper right of each web page.
Up Time	System up time since the last reboot.
Idle Time	System idle time since the last reboot.
Boot	Boot version.
Core	Core version.
Base	Base version.
Program	Program version. This is the main software release version.
Recovery	Recovery version.

NETWORK

Under web GUI->**Status**->**System Status**->**Network**, users could check the network information for the UCM6510. Please see details in the following table.

Table 104: System Status->Network

Status -> System Status -> Network	
MAC Address	Global unique ID of device, in HEX format. The MAC address can be found on the label coming with original box and on the label located on the bottom of the device.
IP Address	IP address.
Gateway	Default gateway address.
Subnet Mask	Subnet mask address.
DNS Server	DNS Server address.

STORAGE USAGE

Users could access the storage usage information from web GUI->**Status**->**System Status**->**Storage Usage**. It shows the available and used space for the following partitions.

- Configuration partition
  This partition contains PBX system configuration files and service configuration files.
- Data partition
  Voicemail, recording files, IVR file, Music On Hold files and etc.
- USB disk
  USB disk will display if connected.
- SD Card
  SD Card will display if connected.

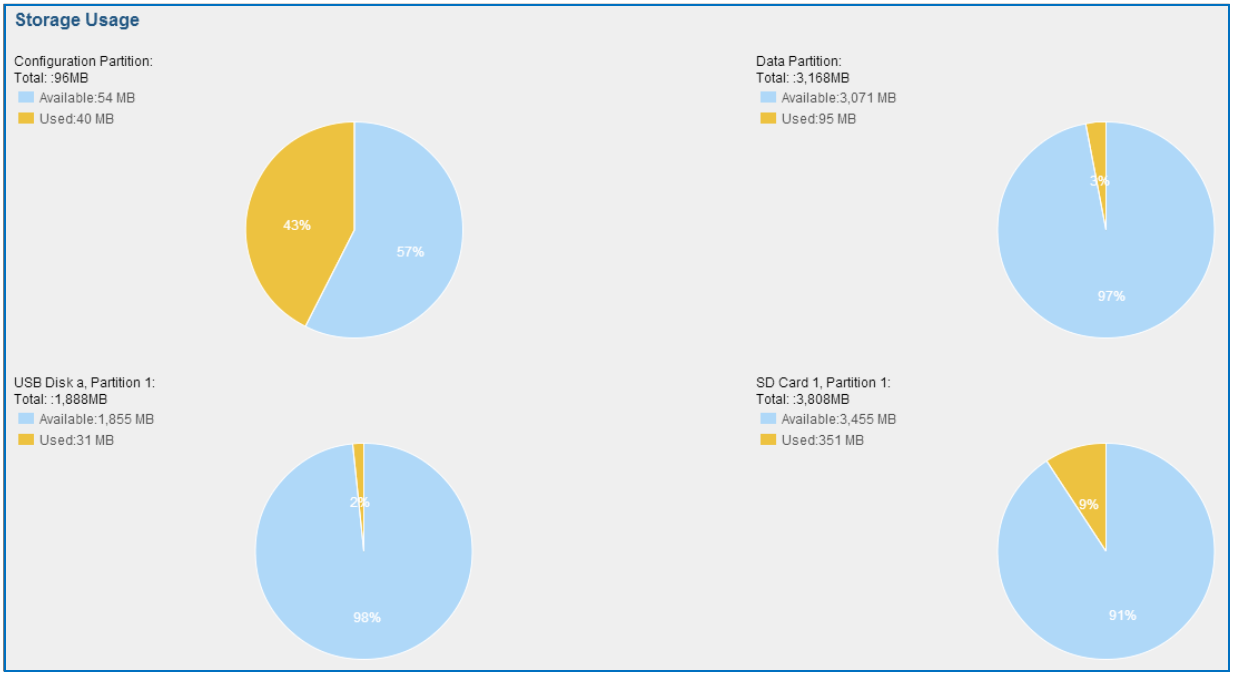


Figure 155: System Status->Storage Usage

RESOURCE USAGE

When configuring and managing the UCM6510, users could access resource usage information to estimate the current usage and allocate the resources accordingly. Under web GUI->**Status**->**System Status**->**Resource Usage**, the current CPU usage and Memory usage are shown in the pie chart.

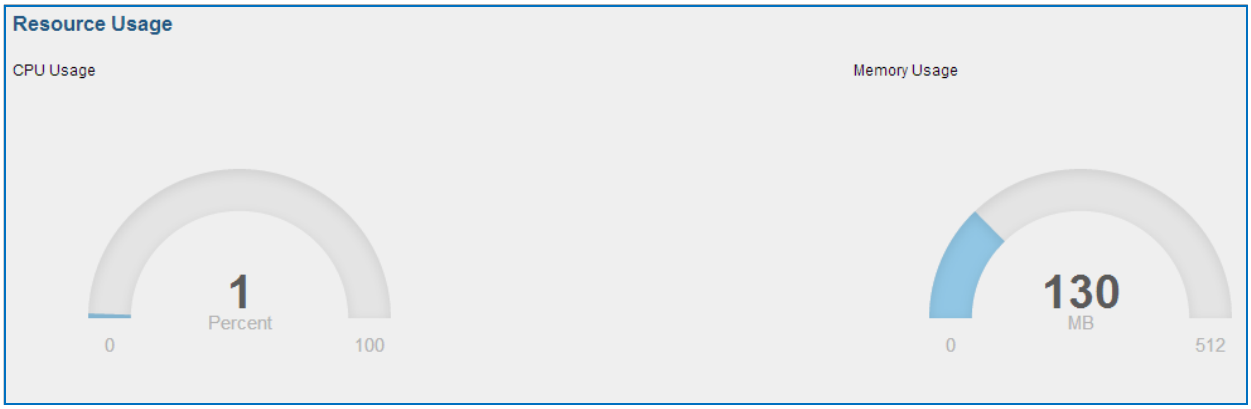


Figure 156: System Status->Resource Usage

SYSTEM EVENTS

The UCM6510 can monitor important system events, log the alerts and send Email notifications to the system administrator.

ALERT EVENTS LIST

The system alert events list can be found under web GUI->**Status**->**System Events**->**Alert Events List**.

Click on to configure the parameters for each event.

1. Disk Usage

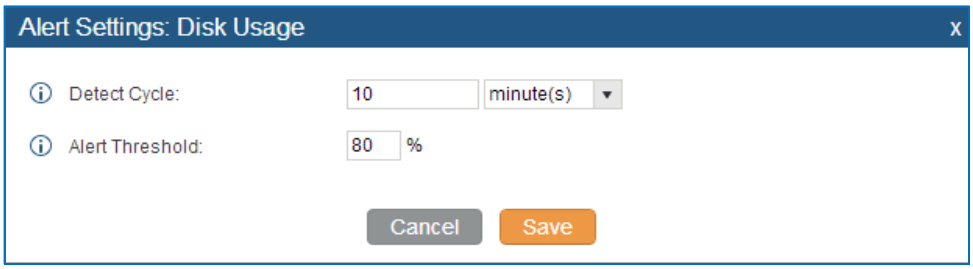


Figure 157: System Events->Alert Events Lists: Disk Usage

- **Detect Cycle**: The UCM6510 will perform the internal disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold**: If the detected value exceeds the threshold (in percentage), the UCM6510 system will send the alert.

2. **Modify Admin Password**

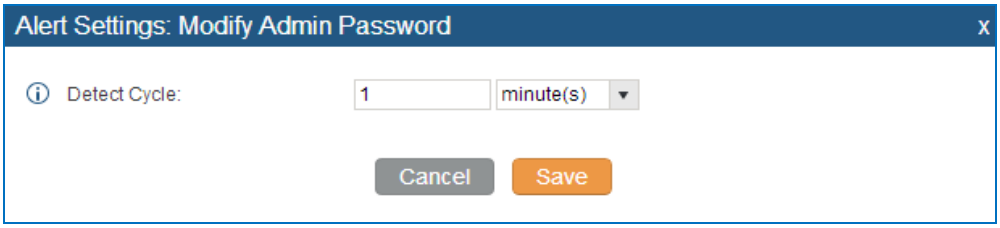


Figure 158: System Events->Alert Events Lists: Modify Admin Password

- **Detect Cycle**: The UCM6510 will initiate the admin password check based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.

3. **Memory Usage**

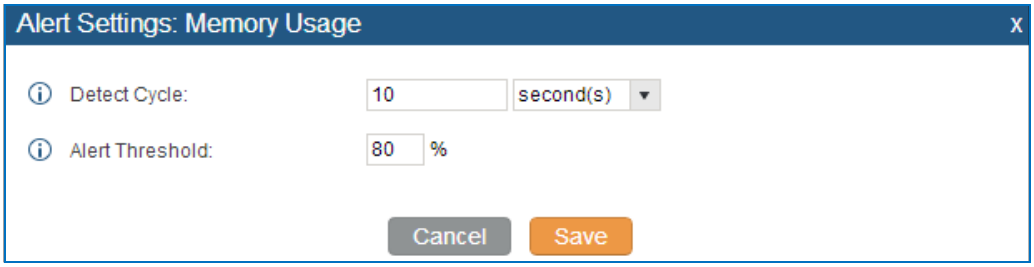


Figure 159: System Events->Alert Events Lists: Memory Usage

- **Detect Cycle**: The UCM6510 will perform the memory usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold**: If the detected value exceeds the threshold (in percentage), the UCM6510 system will send the alert.

4. **System Reboot**

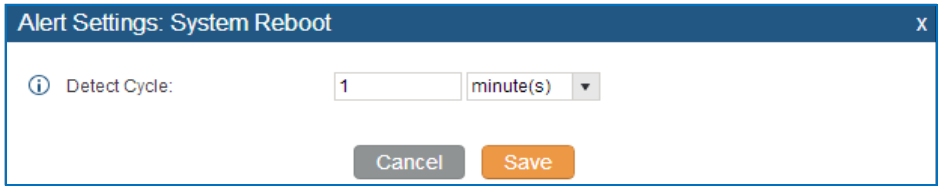


Figure 160: System Events->Alert Events Lists: System Reboot

- **Detect Cycle**: The UCM6510 will check the system reboot based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.

5. **System Update**

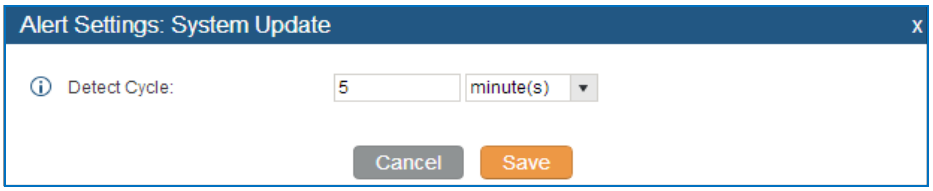


Figure 161: System Events->Alert Events Lists: System Update

- **Detect Cycle**: The UCM6510 will check the system update based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.

6. **System Crash**

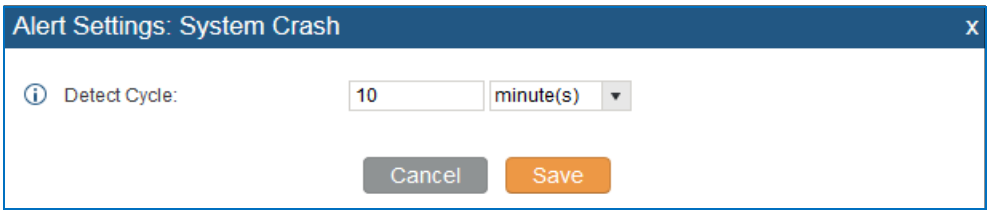


Figure 162: System Events->Alert Events Lists: System Crash

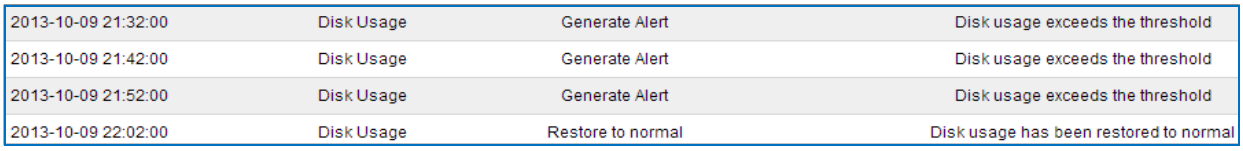
- **Detect Cycle**: The UCM6510 will detect the event at each cycle based on the specified time. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.

Click on the switch

to turn on/off the alert and Email notification for the event. Users could also select the checkbox for each event and then click on button "Alert On", "Alert Off", "Email Notification On", "Email Notification Off" to control the alert and Email notification configuration.

ALERT LOG

Under web GUI->**Status**->**System Events**->**Alert Log**, system messages are listed when the alert is triggered for the configured system events. The following picture shows disk usage alert log. We can tell the detect cycle for the disk usage is 10 minutes and the disk usage is restored to normal after the administrator cleans up the disk storage below the threshold.



2013-10-09 21:32:00	Disk Usage	Generate Alert	Disk usage exceeds the threshold
2013-10-09 21:42:00	Disk Usage	Generate Alert	Disk usage exceeds the threshold
2013-10-09 21:52:00	Disk Usage	Generate Alert	Disk usage exceeds the threshold
2013-10-09 22:02:00	Disk Usage	Restore to normal	Disk usage has been restored to normal

Figure 163: System Events->Alert Log

The following screenshot shows system crash alert logs.

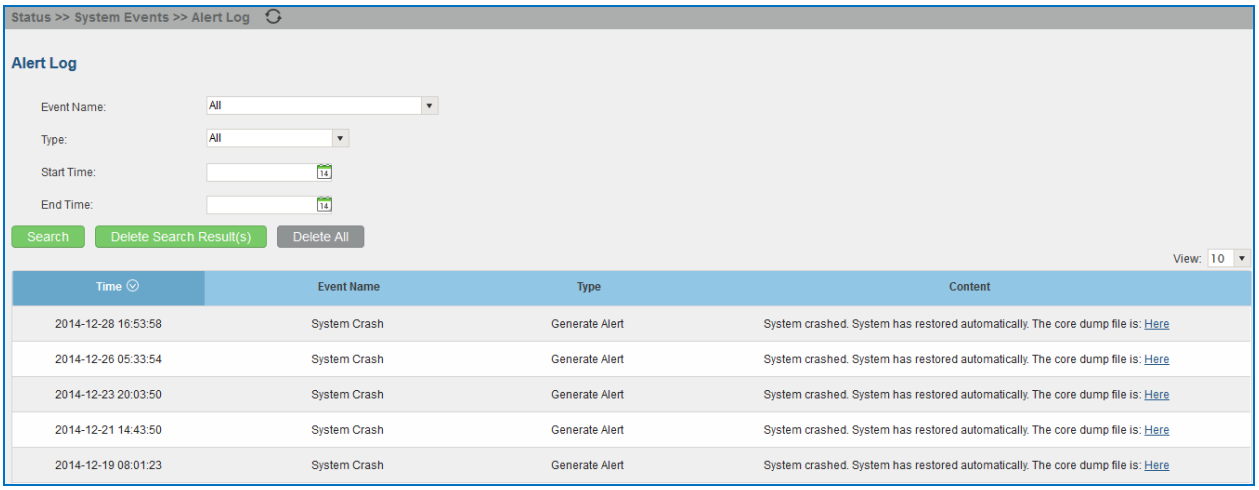

Status >> System Events >> Alert Log
Alert Log
Event Name: All
Type: All
Start Time:
End Time:
Search
Delete Search Result(s)
Delete All
View: 10
Time
Event Name
Type
Content
2014-12-28 16:53:58 System Crash Generate Alert System crashed. System has restored automatically. The core dump file is: Here
2014-12-26 05:33:54 System Crash Generate Alert System crashed. System has restored automatically. The core dump file is: Here
2014-12-23 20:03:50 System Crash Generate Alert System crashed. System has restored automatically. The core dump file is: Here
2014-12-21 14:43:50 System Crash Generate Alert System crashed. System has restored automatically. The core dump file is: Here
2014-12-19 08:01:23 System Crash Generate Alert System crashed. System has restored automatically. The core dump file is: Here

Figure 164: System Events->Alert Log

User could also filter alert logs by selecting a certain event category, type of alert log, and/or specifying a certain time period. The matching results will be displayed after clicking on Search. Alert logs are classified into two types by the system:

1. **Generate Alert:** Generated when alert events happen, for example, alert logs for disk usage exceeding the alert threshold.
2. **Restore to Normal:** Generated when alert events being cleared, for example, logs for disk usage dropping back below the alert threshold.

User could filter out alert logs of “Generate Alert” or “Restore to Normal” by specifying the type according to need. The following figure shows an example of filtering out alert logs of type of “Restore to Normal”.

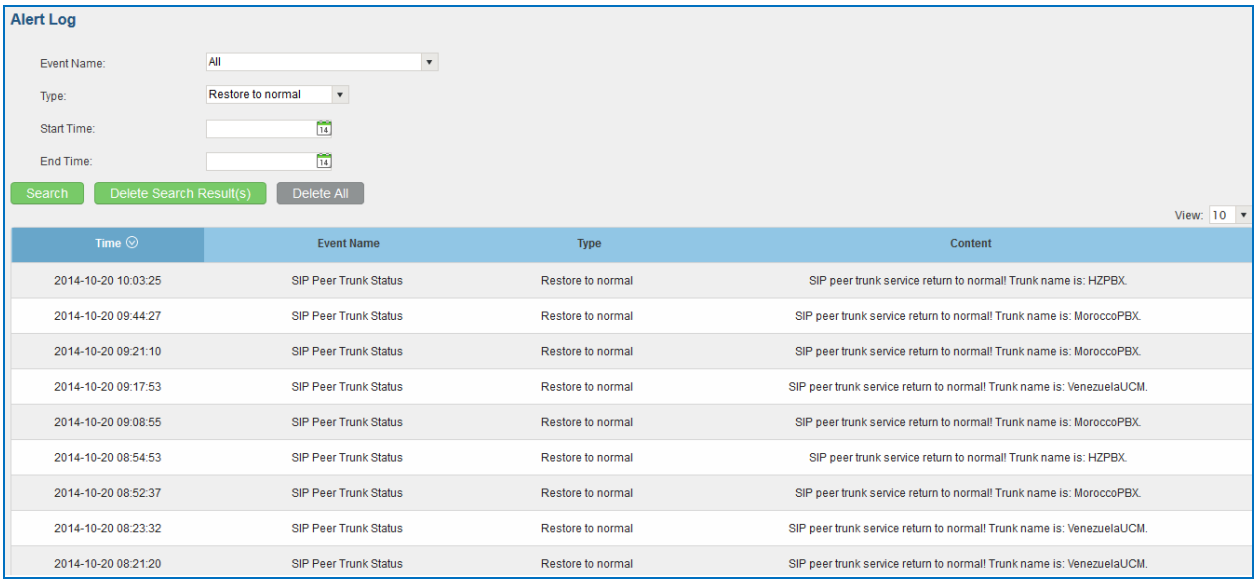

Alert Log
Event Name: All
Type: Restore to normal
Start Time:
End Time:
Search
Delete Search Result(s)
Delete All
View: 10
Time
Event Name
Type
Content
2014-10-20 10:03:25 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: HZPBX.
2014-10-20 09:44:27 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: MoroccoPBX.
2014-10-20 09:21:10 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: MoroccoPBX.
2014-10-20 09:17:53 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: VenezuelaUCM.
2014-10-20 09:08:55 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: MoroccoPBX.
2014-10-20 08:54:53 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: HZPBX.
2014-10-20 08:52:37 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: MoroccoPBX.
2014-10-20 08:23:32 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: VenezuelaUCM.
2014-10-20 08:21:20 SIP Peer Trunk Status Restore to normal SIP peer trunk service return to normal! Trunk name is: VenezuelaUCM.

Figure 165: Filter for Alert Log

ALERT CONTACT

Users could add administrator's Email address under web GUI->**Status**->**System Events**->**Alert Contact** to send the alert notification to. Up to 10 Email addresses can be added.

CDR

A Call Detail Record (CDR) is a data record produced by telephone exchange activities or other telecommunications equipment documenting the details of a phone call that passed through the PBX. The CDR is composed of the following data fields on the UCM6510.

- **Start Time**. Format: 2013-03-27 16:47:03.
- **Call From**. Format: "John Doe"<6012>.
- **Call To**. Format: 6005.
- **Call Time**. Format: 0:00:10.
- **Talk Time**. Format: 0:00:10
- **Status**. Format: NO ANSWER, BUSY, ANSWERED, or FAILED.
- **Options**. Voice record playing/downloading/deleting.

Users could filter the call report by specifying the date range and criteria, depending on how the users would like to include the logs to the report. Then click on "View Report" button to display the generated report.

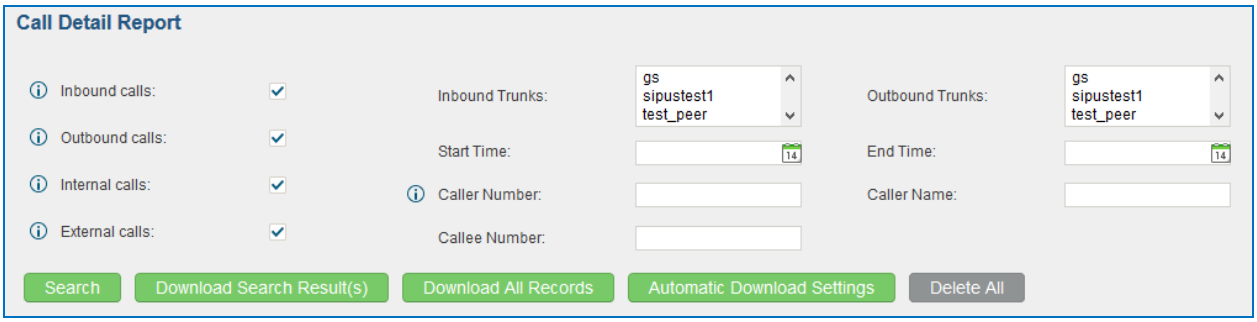


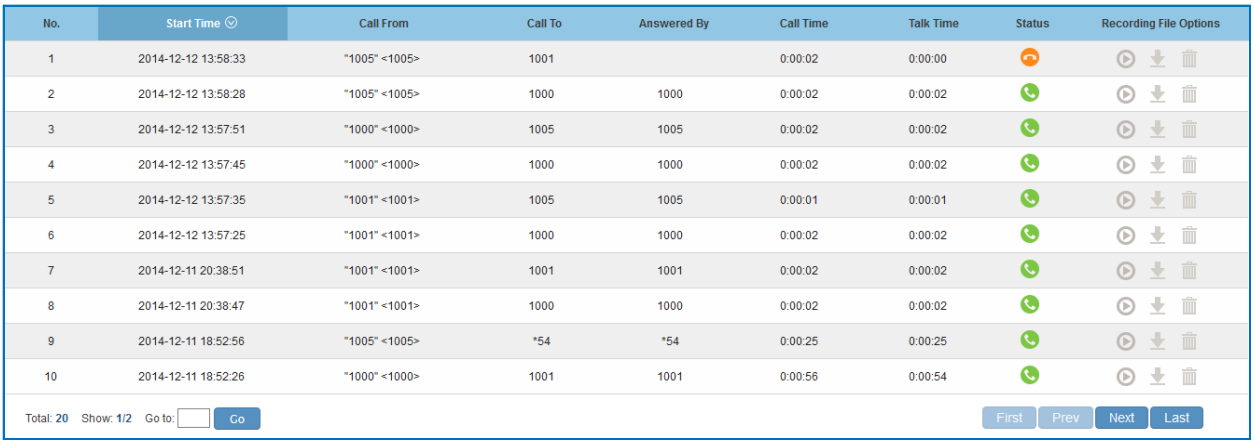
Figure 166: CDR Filter

Table 105: CDR Filter Criteria

Inbound calls	Inbound calls are calls originated from a non-internal source (like a VoIP trunk) and sent to an internal extension.
Outbound calls	Outbound calls are calls sent to a non-internal source (like a VoIP trunk) from an internal extension.
Internal calls	Internal calls are calls from one internal extension to another extension, which are not

	sent over a trunk.
External calls	External calls are calls sent from one trunk to another trunk, which are not sent to any internal extension.
Inbound Trunks	Select certain inbound trunk(s) and the CDR of calls going inbound through the trunk(s) will be filtered out.
Outbound Trunks	Select certain outbound trunk(s) and the CDR of calls going outbound through the trunk(s) will be filtered out.
Caller Number	Enter the caller number to filter the CDR report. CDR with the matching caller number will be filtered out. User could specify a particular caller number or enter a pattern. '.' matches zero or more characters, only appears in the end. 'X' matches any digit from 0 to 9, case-insensitive, repeatable, only appears in the end. For example: 3XXX: It will filter out CDR that having caller number with leading digit 3 and of 4 digits length. 3.: It will filter out CDR that having caller number with leading digit 3 and of any length.
Caller Name	Enter the caller name to filter the CDR report. CDR with the matching caller name will be filtered out.
Callee Number	Enter the callee number to filter the CDR report. CDR with the matching callee number will be filtered out.
Start Time	Specify the start time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.
End Time	Specify the end time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.

The call report will display as the following figure shows.



No.	Start Time	Call From	Call To	Answered By	Call Time	Talk Time	Status	Recording File Options
1	2014-12-12 13:58:33	"1005" <1005>	1001		0:00:02	0:00:00		
2	2014-12-12 13:58:28	"1005" <1005>	1000	1000	0:00:02	0:00:02		
3	2014-12-12 13:57:51	"1000" <1000>	1005	1005	0:00:02	0:00:02		
4	2014-12-12 13:57:45	"1000" <1000>	1000	1000	0:00:02	0:00:02		
5	2014-12-12 13:57:35	"1001" <1001>	1005	1005	0:00:01	0:00:01		
6	2014-12-12 13:57:25	"1001" <1001>	1000	1000	0:00:02	0:00:02		
7	2014-12-11 20:38:51	"1001" <1001>	1001	1001	0:00:02	0:00:02		
8	2014-12-11 20:38:47	"1001" <1001>	1000	1000	0:00:02	0:00:02		
9	2014-12-11 18:52:56	"1005" <1005>	*54	*54	0:00:25	0:00:25		
10	2014-12-11 18:52:26	"1000" <1000>	1001	1001	0:00:56	0:00:54		

Total: 20 Show: 1/2 Go to: Go First Prev Next Last

Figure 167: Call Report

Users could perform the following operations on the call report.

- **Sort**
  Click on the header of the column to sort by this category. For example, clicking on "Start Time" will sort the report according to start time. Clicking on "Start Time" again will reverse the order.
- **Download Records**
  Click on Download Search Result(s) to download the records filtered out or Download All Records to download all records.
- **Delete All**
  On the bottom of the page, click on "Delete All" button to remove all the call report information.
- **Play/Download/Delete Recording File (per entry)**
  If the entry has audio recording file for the call, the three icons on the most right column will be activated for users to select. In the following picture, the second entry has audio recording file for the call.

  Click on to play the recording file; click on to download the recording file in .wav format; click on to delete the recording file (the call record entry will not be deleted).

Figure 168: Call Report Entry with Audio Recording File

- **Automatic Download CDR Records**
  User could configure the UCM6510 to automatically download the CDR records and send the records to an Email address. Click on “Automatic Download Settings”, and configure the parameters in the dialog below.

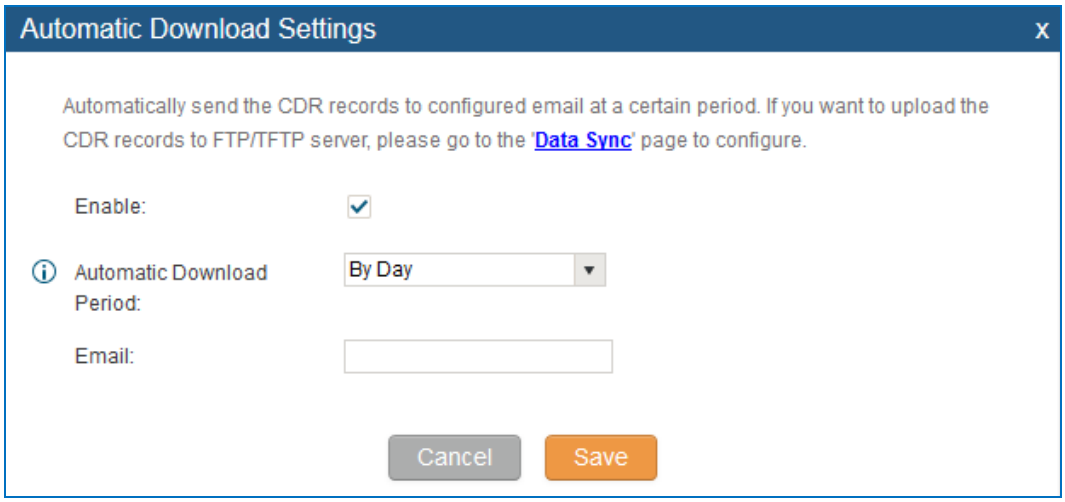

Automatic Download Settings
x
Automatically send the CDR records to configured email at a certain period. If you want to upload the CDR records to FTP/TFTP server, please go to the 'Data Sync' page to configure.
Enable:
Automatic Download Period:
By Day
Email:
Cancel
Save

Figure 169: Automatic Download Settings

To receive CDR record automatically from Email, check “Enable” and select a time period “By Day” “By Week” or “By Month” for the automatic download period. Make sure you have entered an Email address to receive the CDR records.

DOWNLOADED CDR FILE

The downloaded CDR (.csv file) has different format from the web UI CDR. Here are some descriptions.

- **Call From, Call To**

"Call From": the caller ID.
"Call To": the callee ID.

If "Call From" shows empty, "Call To" shows "s" (see highlight part in the picture below) and the "Source Channel" contains "DAHDI", this means the call is from FXO/PSTN line. For FXO/PSTN line, we only know there is an incoming request when there is incoming call but we don't know the number being called. So we are using "s" to match it where "s" means "start".

call from	call to	context	start time	answer time	end time	call time	talk time	source channel	dest channel	status
610	19097622990	from-internal	1/29/2014 14:28	1/29/2014 14:28	1/29/2014 14:31	153	150	SIP/610-00000074	DAHDI/1-1	ANSWERED
	s	default	1/29/2014 14:33		1/29/2014 14:33	8	0	DAHDI/pseudo-149089967		NO ANSWER
	s	default	1/29/2014 14:33		1/29/2014 14:33	9	0	DAHDI/pseudo-1067045536		NO ANSWER
601	688	from-internal	1/29/2014 14:33	1/29/2014 14:33	1/29/2014 14:33	9	9	SIP/601-00000077		ANSWERED
	s	default	1/29/2014 14:34		1/29/2014 14:34	22	0	DAHDI/pseudo-1124093033		NO ANSWER
	s	default	1/29/2014 14:34		1/29/2014 14:34	22	0	DAHDI/pseudo-1719498666		NO ANSWER

Figure 170: Downloaded CDR File Sample - Call To Shows "s"

- **Context**

There are different context values that might show up in the downloaded CDR file. The actual value can vary case by case. Here are some sample values and their descriptions.

from-internal: internal extension makes outbound calls.
ext-did-XXXXX: inbound calls. It starts with "ext-did", and "XXXXX" content varies case by case, which also relate to the order when the trunk is created.
ext-local: internal calls between local extensions.

- **Source Channel, Dest Channel**

Sample 1:

call from	call to	context	start time	answer time	end time	call time	talk time	source channel	dest channel	status
3122731439	s	ext-did-1	1/30/2014 14:27	1/30/2014 14:27	1/30/2014 14:27	37	35	DAHDI/1-1		ANSWERED

Figure 171: Downloaded CDR File Sample - Source Channel and Dest Channel 1

DAHDI means it is an analog call, FXO or FXS.
For UCM6510, DAHDI/(1-2) are FXO ports, and DAHDI(3-4) are FXS ports.
For UCM6510, DAHDI/(1-4) are FXO ports, and DAHDI(5-6) are FXS ports.
For UCM6510, DAHDI/(1-8) are FXO ports, and DAHDI(9-10) are FXS ports.
For UCM6510, DAHDI/(1-16) are FXO ports, and DAHDI/(17-18) are FXS ports.

Sample 2:

call from	call to	context	start time	answer time	end time	call time	talk time	source channel	dest channel	status
609	619	from-internal	1/30/2014 14:31	1/30/2014 14:32	1/30/2014 14:32	9	3	SIP/609-00000150	SIP/619-00000151	ANSWERED

Figure 172: Downloaded CDR File Sample - Source Channel and Dest Channel 2

"SIP" means it's a SIP call. There are three possible format:
(a) **SIP/NUM-XXXXXX,** where NUM is the local SIP extension number. The last XXXXX is a random string and can be ignored.
(c) **SIP/trunk_X/NUM,** where trunk_X is the internal trunk name, and NUM is the number to dial out through the trunk.
(c) **SIP/trunk_X-XXXXXX,** where trunk_X is the internal trunk name and it is an inbound call from this trunk. The last XXXXX is a random string and can be ignored.

Sample 3:

call from	call to	context	start time	answer time	end time	call time	talk time	source channel	dest channel	status
	s	default	1/30/2014 14:30		1/30/2014 14:37	386	0	DAHDI/pseudo-1665832080		NO ANSWER
	s	default	1/30/2014 14:30		1/30/2014 14:37	390	0	DAHDI/pseudo-1946772436		NO ANSWER

Figure 173: Downloaded CDR File Sample - Source Channel and Dest Channel 3

This is a very special channel name. If it shows up, most likely it means a conference call.

There are some other possible values, but these values are almost the application name which are used by the dialplan.

IAX2/NUM-XXXXXXX: it means this is an IAX call.
Local/@from-internal-XXXXX: it is used internally to do some special feature procedure. We can simply ignore it.
Hangup: the call is hung up from the dialplan. This indicates there are some errors or it has run into abnormal cases.
Playback: play some prompts to you, such as 183 response or run into an IVR.
ReadExten: collect numbers from user. It may occur when you input PIN codes or run into DISA

STATISTICS

CDR Statistics is an additional feature on the UCM6510 which provides users a visual overview of the call report across the time frame. Users can filter with different criteria to generate the statistics chart.

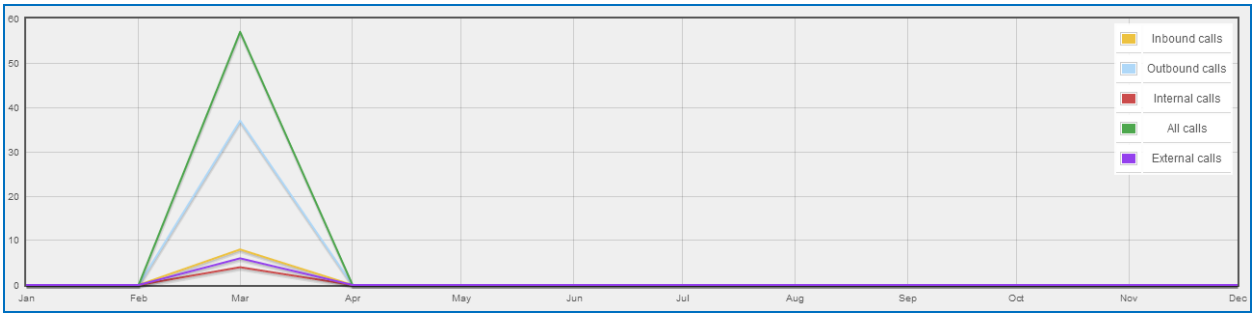


Figure 174: CDR Statistics

Table 106: CDR Statistics Filter Criteria

Trunk Type	Select one of the following trunk type. • All • SIP Calls • PSTN Calls
Call Type	Select one or more in the following checkboxes. • Inbound calls • Outbound calls • Internal calls • External calls • All calls
Time Range	• By month (of the selected year). • By week (of the selected year). • By day (of the specified month for the year). • By hour (of the specified date). • By range. For example, 2013-01 To 2013-03.

RECORDING FILES

The recording files recorded by "Auto Record" per extension/per trunk, or via feature code "Audio Mix Record" are listed here. Users could click on to play the recording file; click on to download the recording file in .wav format; click on to delete the recording file; or click on

Delete Selected Recording Files or Delete All Recording Files to delete multiple recording files at one click.

To sort the recording file, click on the title "Caller", "Callee" or "Call Time" for the corresponding column. Click on the title again can switch the sorting mode between ascending order and descending order.

CDR API CONFIGURATION FILES

The UCM6510 supports third party billing interface API for external billing software to access CDR on the PBX. The API uses HTTPS to request the CDR data matching given parameters as configured on the third party application. Before accessing the API, the administrators need enable API and configure the access/authentication information on the UCM6510 first.

Table 107: CDR API Configuration Files

Enable	Enable/Disable CDR API. The default setting is disabled.
TLS Bind Address	Configure the IP address for TLS server to bind to. "0.0.0.0" means binding to all interfaces. The port number is optional and the default port number is 8443. The IP address must match the common name (host name) in the certificate so that the TLS socket won't bind to multiple IP addresses. The default setting is 0.0.0.0:8443.
TLS Private Key	Upload TLS private key. The size of the key file must be under 2MB. This file will be renamed as 'private.pem' automatically.
TLS Cert	Upload TLS cert. The size of the certificate must be under 2MB. This is the certificate file (*.pem format only) for TLS connection. This file will be renamed as "certificate.pem" automatically. It contains private key for the client and signed certificate for the server.
TLS Authentication Name	Configure the user name for TLS authentication. If not configured, authentication will be skipped.
TLS Authentication Password	Configure the password for TLS authentication. This is optional.
Permitted	Specify a list of IP addresses permitted by CDR API. This creates an AIP-specific access control list. Multiple entries are allowed. For example, "192.168.40.3/255.255.255.255" denies access from all IP addresses except 192.168.40.3.

The format of the HTTPS request for the CDR API is as below.

https://[UCM IP]:[Port]/cdrapi?[option1]=[value]&[option2]=[value]&...

By default, the port number for the API is 8443.

The options included in the request URI control the record matching and output format. For CDR matching parameters, all non-empty parameters must have a match to return a record. Parameters can appear in the URI in any order. Multiple values given for caller or callee will be concatenated. The following table shows the parameter list used in the CDR API.

Table 108: CDR API URI Parameters

Field	Value	Details
format	csv, xml, json	Define the format for output of matching CDR rows. Default is csv (comma separated values).
numRecords	Number: 0-1000	Number of records to return. Default is 1000, which is also the maximum allowed value.
offset	Number	Number of matching records to skip. This will be combined with numRecords to receive all matches over multiple responses. Default is 0.
caller callee	Comma separated extensions, ranges of extensions, or regular expressions. Example: caller=5300,5302-5304,_4@ -OR- caller=5300&caller=5302-5304&caller=_4@ (Matches extensions 5300, 5302, 5303, 5304, and any extension containing 4 as the second digit/character).	Filters based on src (caller) or dst (callee) value, matching any extension contained in the parameter input string. Patterns containing one or more wildcards ('@' or '_') will match as a regular expression, and treat '-' as a literal hyphen rather than a range signifier. The '@' wildcard matches any number of characters (including zero), while '_' matches any single character. Otherwise, patterns containing a single hyphen will be matching a range of numerical extensions, with non-numerical characters ignored, while patterns containing multiple hyphens will be ignored. (The pattern "0-0" will match all non-numerical and empty strings).
startTime endTime	Date and/or time of day in any of the following formats: YYYY-MM-DDTHH:MM	Filters based on the start (call start time) value. Calls which start within this period (inclusive of boundaries) will match, regardless of the call answer or end time. An empty value for either field will be interpreted as range with no minimum or maximum respectively.

	YYYY-MM-DDTHH:MM:SS YYYY-MM-DDTHH:MM:SS.SSS (literal 'T' character separator in above three formats) HH:MM HH:MM:SS HH:MM:SS.SSS now DDDDDDDDDD	Strings without a date have a default value of 2000-01-01. Strings without a time of day have a default value of of 00:00 UTC, while strings with a time of day specified may also optionally specify a time zone offset - replace '+' in time zone offset with '%2B' (see http://www.w3.org/TR/NOTE-datetime).
minDur	Number (duration in seconds)	Filters based on the billsec value, the duration between call answer and call end.
maxDur		

Example Queries:

The following illustrates the format of queries to accomplish certain requests. In most cases, multiple different queries will accomplish the same goal, and these examples are not intended to be exhaustive, but rather to bring attention to particular features of the CDR API connector.

Query 1: Request all records of calls placed on extension 5300 which last between 8 and 60 seconds (inclusive), with results in CSV format.

https://192.168.254.200:8088/cdrapi?format=CSV&caller=5300&minDur=8&maxDur=60

-OR-

https://192.168.254.200:8088/cdrapi?caller=5300&minDur=8&maxDur=60

Query 2: Request all records of calls placed on extension 5300 or in the range 6300-6399 to extensions starting with 5, with results in XML format.

https://192.168.254.200:8088/cdrapi?format=XML&caller=5300,6300-6399&callee=5@

-OR-

https://192.168.254.200:8088/cdrapi?cdrapi?format=XML&caller=5300&caller=6300-6399&callee=5@

Query 3: Request all records of calls placed on extensions containing substring "53" prior to January 23, 2013 00:00:00 UTC to extensions 5300-5309, with results in CSV format.

https://192.168.254.200:8088/cdrapi?caller=@53@&callee=5300-5309&endTime=2013-01-23

-OR-

https://192.168.254.200:8088/cdrapi?caller=@53@&callee=530_&endTime=2013-01-23T00:00:00

Query 4: Request all records of calls placed by an Anonymous caller during July 2013 Central Standard Time to extensions starting with 2 or 34 or ending with 5, with results in CSV format.

https://192.168.254.200:8088/cdrapi?caller=Anonymous&callee=2@,34@,@5&startTime=2013-07-01T00:00:00-06:00&endTime=2013-07-31T23:59:59-06:00

Query 5: Request all records during July 2013 Central Standard Time, 200 at a time, with results in CSV format.

https://192.168.254.200:8088/cdrapi?startTime=2013-07-01T00:00:00-06:00&endTime=2013-07-31T23:59:59-06:00&numRecords=200&offset=0

-THEN-

https://192.168.254.200:8088/cdrapi?sstartTime=2013-07-01T00:00:00-06:00&endTime=2013-07-31T23:59:59-06:00&numRecords=200&offset=200

-THEN-

https://192.168.254.200:8088/cdrapi?startTime=2013-07-01T00:00:00-06:00&endTime=2013-07-31T23:59:59-06:00&numRecords=200&offset=400

⚠ **Note:**

- Disallowed characters in the caller, callee, startTime, or endTime strings, and non-digit characters in the values of numRecords, offset, minDur, or maxDur, will result in no records returned - the appropriate container/header for the output format will be the only output. If the format parameter is in error, the CSV header will be used. Error messages will appear in the Asterisk log (along with errors stemming from failed database connections, etc.).
- Other errors which return no records include:

  - Multiple hyphens in an extension range (e.g. caller=5300-5301-,6300)

  - Empty parameter value (e.g. caller=)

  - Extension values starting with comma, or with consecutive commas (e.g. caller=5300,,5303)

  - Unknown parameters (e.g. caler=5300) or URI ending with '&'

  - Except for caller and callee, multiple instances of the same parameter within the URI (e.g. minDur=5&minDur=10)

Example Output:

The following are examples of each of the output formats for the same data set.

CSV:

```
AcctId,accountcode,src,dst,dcontext,clid,channel,dstchannel,lastapp,lastdata,start,answer,end,duration,
billsec,disposition,amaflags,uniqueid,userfield,channel_ext,dstchannel_ext,service
62,,5300,5301,from-internal,"pn01"
<5300>,SIP/5300-00000000,SIP/5301-00000001,Dial,SIP/5301,60,,2013-12-03 11:46:40,2013-12-03
11:46:43,2013-12-03 11:46:49,9,6,ANSWERED,DOCUMENTATION,1386092800.0,EXT,5300,5301,s
63,,5300,5301,from-internal,"pn01"
<5300>,SIP/5300-00000000,SIP/5301-00000001,Dial,SIP/5301,60,,2013-12-03 14:01:41,2013-12-03
14:01:43,2013-12-03 14:01:46,5,3,ANSWERED,DOCUMENTATION,1386100901.0,EXT,5300,5301,s
64,,5300,5301,from-internal,"pn01"
<5300>,SIP/5300-00000002,SIP/5301-00000003,Dial,SIP/5301,60,,2013-12-03 14:02:23,2013-12-03
14:02:27,2013-12-03 14:02:31,8,4,ANSWERED,DOCUMENTATION,1386100943.2,EXT,5300,5301,s
```

XML:

```
<root>
<cdr><AcctId>62</AcctId><accountcode></accountcode><src>5300</src><dst>5301</dst><dcontext
>from-internal</dcontext><clid>&amp;quot;pn01&amp;quot;
&amp;lt;5300&amp;gt;</clid><channel>SIP/5300-00000000</channel><dstchannel>SIP/5301-00000001</dstcha
nnel><lastapp>Dial</lastapp><lastdata>SIP/5301,60,</lastdata><start>2013-12-03
11:46:40</start><answer>2013-12-03 11:46:43</answer><end>2013-12-03
11:46:49</end><duration>9</duration><billsec>6</billsec><disposition>ANSWERED</disposition><a
maflags>DOCUMENTATION</amaflags><uniqueid>1386092800.0</uniqueid><userfield>EXT</userfie
ld><channel_ext>5300</channel_ext><dstchannel_ext>5301</dstchannel_ext><service>s</service></
cdr>
<cdr><AcctId>63</AcctId><accountcode></accountcode><src>5300</src><dst>5301</dst><dcontext
>from-internal</dcontext><clid>&amp;quot;pn01&amp;quot;
&amp;lt;5300&amp;gt;</clid><channel>SIP/5300-00000000</channel><dstchannel>SIP/5301-00000001</dstcha
nnel><lastapp>Dial</lastapp><lastdata>SIP/5301,60,</lastdata><start>2013-12-03
14:01:41</start><answer>2013-12-03 14:01:43</answer><end>2013-12-03
14:01:46</end><duration>5</duration><billsec>3</billsec><disposition>ANSWERED</disposition><a
maflags>DOCUMENTATION</amaflags><uniqueid>1386100901.0</uniqueid><userfield>EXT</userfie
ld><channel_ext>5300</channel_ext><dstchannel_ext>5301</dstchannel_ext><service>s</service></
cdr>
<cdr><AcctId>64</AcctId><accountcode></accountcode><src>5300</src><dst>5301</dst><dcontext
>from-internal</dcontext><clid>&amp;quot;pn01&amp;quot;
&amp;lt;5300&amp;gt;</clid><channel>SIP/5300-00000002</channel><dstchannel>SIP/5301-00000003</dstcha
nnel><lastapp>Dial</lastapp><lastdata>SIP/5301,60,</lastdata><start>2013-12-03
14:02:23</start><answer>2013-12-03 14:02:27</answer><end>2013-12-03
14:02:31</end><duration>8</duration><billsec>4</billsec><disposition>ANSWERED</disposition><a
maflags>DOCUMENTATION</amaflags><uniqueid>1386100943.2</uniqueid><userfield>EXT</userfie
ld><channel_ext>5300</channel_ext><dstchannel_ext>5301</dstchannel_ext><service>s</service></
cdr>
</root>
```

JSON:

```
{
    "cdr":
    [
        { "AcctId": "62", "accountcode": "", "src": "5300", "dst": "5301", "dcontext": "from-internal", "clid":
"\"pn01\" <5300>", "channel": "SIP/5300-00000000", "dstchannel": "SIP/5301-00000001", "lastapp":
"Dial", "lastdata": "SIP/5301,60,", "start": "2013-12-03 11:46:40", "answer": "2013-12-03 11:46:43",
"end": "2013-12-03 11:46:49", "duration": "9", "billsec": "6", "disposition": "ANSWERED", "amaflags":
"DOCUMENTATION", "uniqueid": "1386092800.0", "userfield": "EXT", "channel_ext": "5300",
"dstchannel_ext": "5301", "service": "s" },
        { "AcctId": "63", "accountcode": "", "src": "5300", "dst": "5301", "dcontext": "from-internal", "clid":
"\"pn01\" <5300>", "channel": "SIP/5300-00000000", "dstchannel": "SIP/5301-00000001", "lastapp":
"Dial", "lastdata": "SIP/5301,60,", "start": "2013-12-03 14:01:41", "answer": "2013-12-03 14:01:43",
"end": "2013-12-03 14:01:46", "duration": "5", "billsec": "3", "disposition": "ANSWERED", "amaflags":
"DOCUMENTATION", "uniqueid": "1386100901.0", "userfield": "EXT", "channel_ext": "5300",
"dstchannel_ext": "5301", "service": "s" },
        { "AcctId": "64", "accountcode": "", "src": "5300", "dst": "5301", "dcontext": "from-internal", "clid":
"\"pn01\" <5300>", "channel": "SIP/5300-00000002", "dstchannel": "SIP/5301-00000003", "lastapp":
"Dial", "lastdata": "SIP/5301,60,", "start": "2013-12-03 14:02:23", "answer": "2013-12-03 14:02:27",
"end": "2013-12-03 14:02:31", "duration": "8", "billsec": "4", "disposition": "ANSWERED", "amaflags":
"DOCUMENTATION", "uniqueid": "1386100943.2", "userfield": "EXT", "channel_ext": "5300",
"dstchannel_ext": "5301", "service": "s" }
    ]
}
```

This page intentionally left blank

UPGRADING AND MAINTENANCE

UPGRADING

The UCM6510 can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your UCM6510 via network or local upload.

UPGRADING VIA NETWORK

The UCM6510 can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP or HTTPS; the server name can be FQDN or IP address.

Examples of valid URLs:
firmware.grandstream.com

The upgrading configuration can be accessed via **web GUI**->**Maintenance**->**Upgrade**.

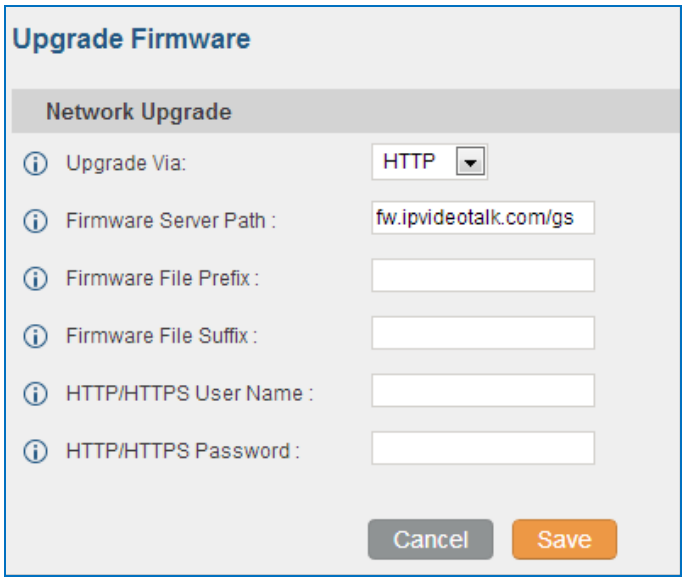


Figure 175: Network Upgrade

Table 109: Network Upgrade Configuration

Upgrade Via	Allow users to choose the firmware upgrade method: TFTP, HTTP or HTTPS.
Firmware Server Path	Define the server path for the firmware server.

Firmware File Prefix	If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the UCM6510.
Firmware File Suffix	If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the UCM6510.
HTTP/HTTPS User Name	The user name for the HTTP/HTTPS server.
HTTP/HTTPS Password	The password for the HTTP/HTTPS server.

Please follow the steps below to upgrade the firmware remotely.

- Enter the firmware server path under **web GUI**->**Maintenance**->**Upgrade**.
- Click on "Save". Then reboot the device to start the upgrading process.
- Please be patient during the upgrading process. Once done, a reboot message will be displayed in the LCD.
- Manually reboot the UCM6510 when it's appropriate to avoid immediate service interruption. After it boots up, log in the web GUI to check the firmware version.

UPGRADING VIA LOCAL UPLOAD

If there is no HTTP/TFTP server, users could also upload the firmware to the UCM6510 directly via web GUI. Please follow the steps below to upload firmware locally.

1. Download the latest UCM6510 firmware file from the following link and save it in your PC. http://www.grandstream.com/support/firmware

2. Log in the web GUI as administrator in the PC.
3. Go to web GUI->**Maintenance**->**Upgrade**, upload the firmware file by clicking on and select the firmware file from your PC. The default firmware file name is ucm6510fw.bin

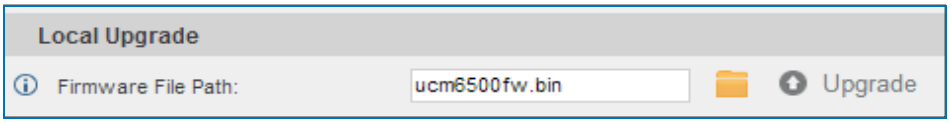


Figure 176: Local Upgrade

4. Click on to start upgrading.

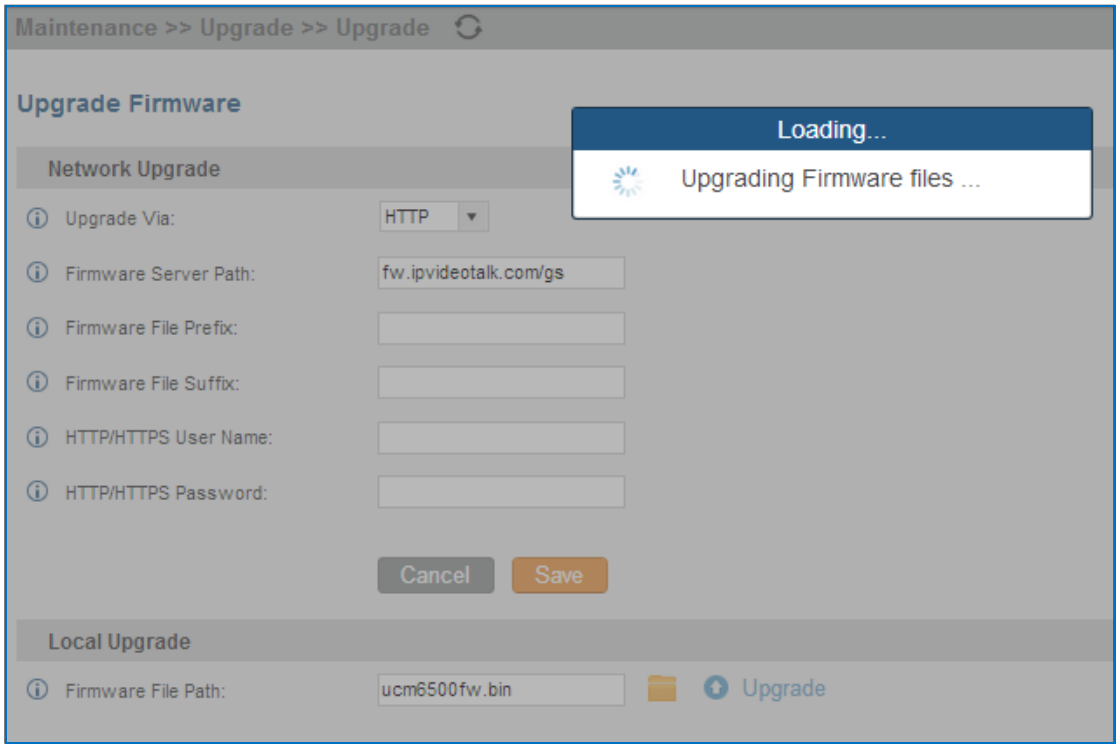


Figure 177: Upgrading Firmware Files

5. Wait until the upgrading process is successful and a window will be popped up in the web GUI.

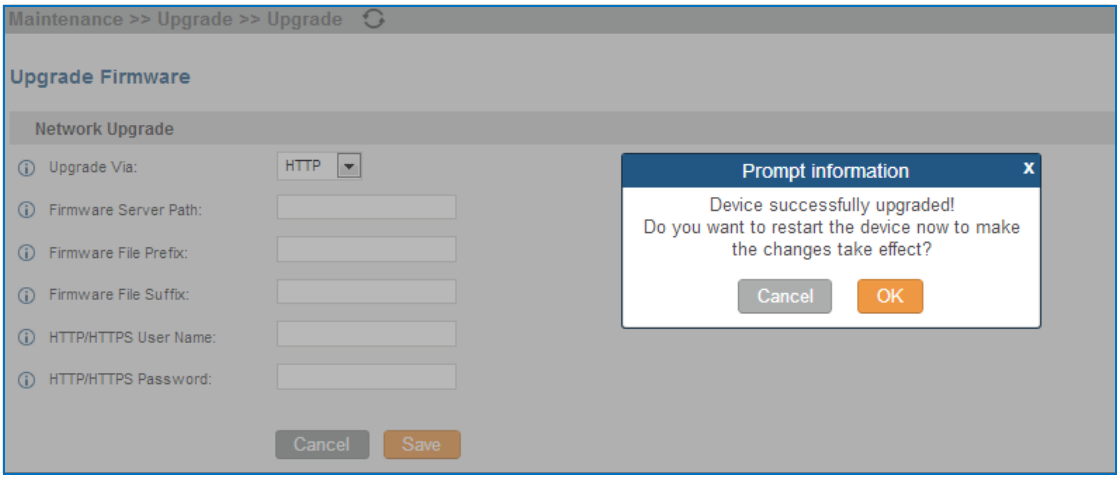


Figure 178: Reboot UCM6510

6. Click on "OK" to reboot the UCM6510 and check the firmware version after it boots up.

⚠ **Note:**

Please do not interrupt or power cycle the UCM6510 during upgrading process.

NO LOCAL FIRMWARE SERVERS

For users that would like to use remote upgrading without a local TFTP server, Grandstream offers a NAT-friendly HTTP server. This enables users to download the latest software upgrades for their devices via this server. Please refer to the webpage:
http://www.grandstream.com/support/firmware.

Alternatively, users can download a free TFTP or HTTP server and conduct a local firmware upgrade. A free windows version TFTP server is available for download from:
http://www.solarwinds.com/products/freetools/free_tftp_server.aspx
http://tftpd32.jounin.net

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server;
2. Connect the PC running the TFTP server and the UCM6510 to the same LAN segment;
3. Launch the TFTP server and go to the File menu->Configure->Security to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade;
4. Start the TFTP server and configure the TFTP server in the UCM6510 web configuration interface;
5. Configure the Firmware Server Path to the IP address of the PC;
6. Update the changes and reboot the UCM6510.

End users can also choose to download a free HTTP server from http://httpd.apache.org/ or use Microsoft IIS web server.

BACKUP

The UCM6510 configuration can be backed up locally or via network. The backup file will be used to restore the configuration on UCM6510 when necessary.

BACKUP/RESTORE

Users could backup the UCM6510 configurations for restore purpose under web GUI->**Maintenance**->**Backup**->**Backup / Restore**. Click on Create New Backup to create a new backup. Then the following dialog will show.

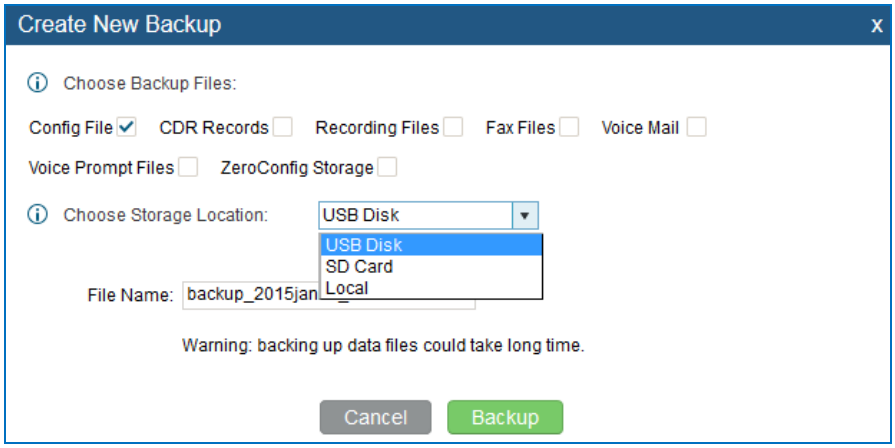


Figure 179: Create New Backup

1. Choose the files to be included in the backup.
2. Choose where to store the backup file: USB Disk, SD Card or Local.
3. Name the backup file.
4. Click on "Backup" to start backup.

Once the backup is done, the list of the backups will be displayed with date and time in the web page. Users can download, restore, or delete it from the UCM6510 internal storage or the external device.

Click on Upload Backup File to upload backup file from the local device to UCM6510. The uploaded backup file will also be displayed in the web page and can be used to restore the UCM6510.

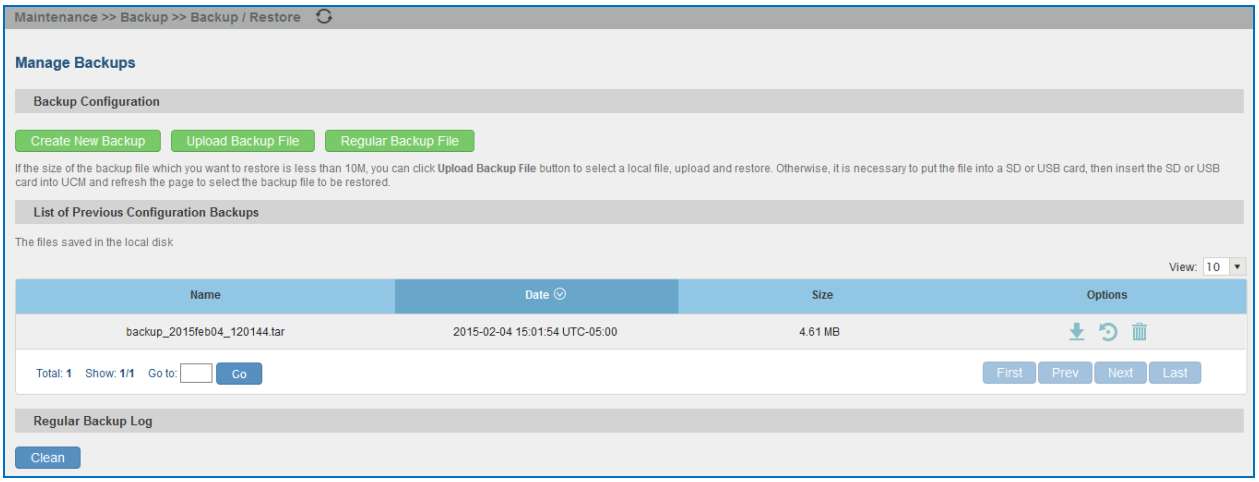

Maintenance >> Backup >> Backup / Restore
Manage Backups
Backup Configuration
Create New Backup
Upload Backup File
Regular Backup File
If the size of the backup file which you want to restore is less than 10M, you can click Upload Backup File button to select a local file, upload and restore. Otherwise, it is necessary to put the file into a SD or USB card, then insert the SD or USB card into UCM and refresh the page to select the backup file to be restored.
List of Previous Configuration Backups
The files saved in the local disk
View: 10
Name
Date
Size
Options
backup_2015feb04_120144.tar
2015-02-04 15:01:54 UTC-05:00
4.61 MB
Total: 1 Show: 1/1 Go to: Go
First Prev Next Last
Regular Backup Log
Clean

Figure 180: Backup / Restore

Regular Backup File option allows UCM6510 to perform automatically backup on the user specified time. Regular backup file can only be stored in USB / SD card / SFTP server. User is allowed to set backup time from 0-23 and how frequent the backup will be performed.

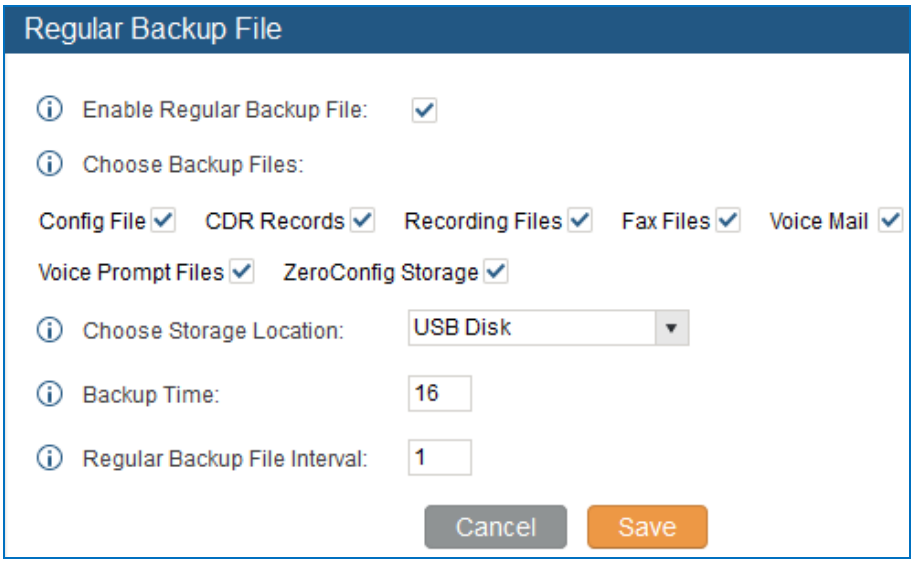


Figure 181: Local Backup

DATA SYNC

Besides local backup, users could backup the voice records/voice mails/CDR/FAX in a daily basis to a remote server via SFTP protocol automatically under web GUI->**Maintenance**->**Backup**->**Data Sync**.

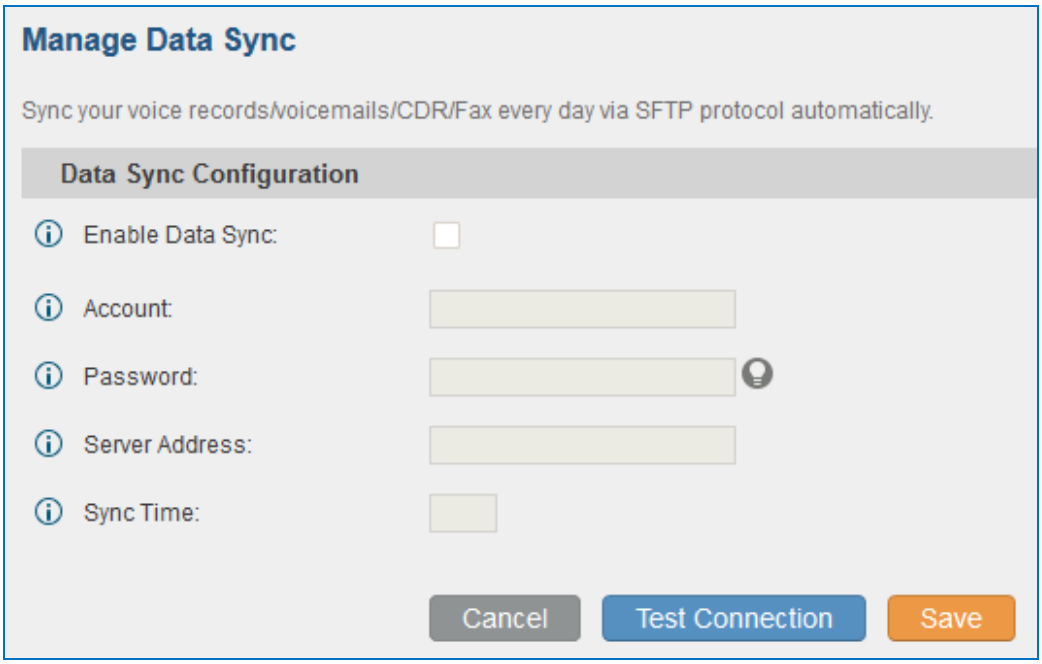


Figure 182: Data Sync

Table 110: Data Sync Configuration

Enable Backup	Enable the auto backup function. The default setting is "No".
Account	Enter the Account name on the SFTP backup server.
Password	Enter the Password associate with the Account on the SFTP backup server.
Server Address	Enter the SFTP server address.
Backup Time	Enter 0-23 to specify the backup hour of the day.

Before saving the configuration, users could click on "Test Connection". The UCM6510 will then try connecting the server to make sure the server is up and accessible for the UCM6510.

Save the changes and all the backup logs will be listed on the web page.

RESTORE CONFIGURATION FROM BACKUP FILE

To restore the configuration on the UCM6510 from a backup file, users could go to web GUI->**Maintenance**->**Backup**->**Backup / Restore**.

- A list of previous configuration backups is displayed on the web page. Users could click on of the desired backup file and it will be restored to the UCM6510.

- If users have other backup files on PC to restore on the UCM6510, click on "Upload Backup File" first and select it from local PC to upload on the UCM6510. Once the uploading is done, this backup file will be displayed in the list of previous configuration backups for restore purpose. Click on to restore from the backup file.
- User could also restore using the backup file saved in SD card or USB device plugged into the UCM6510.

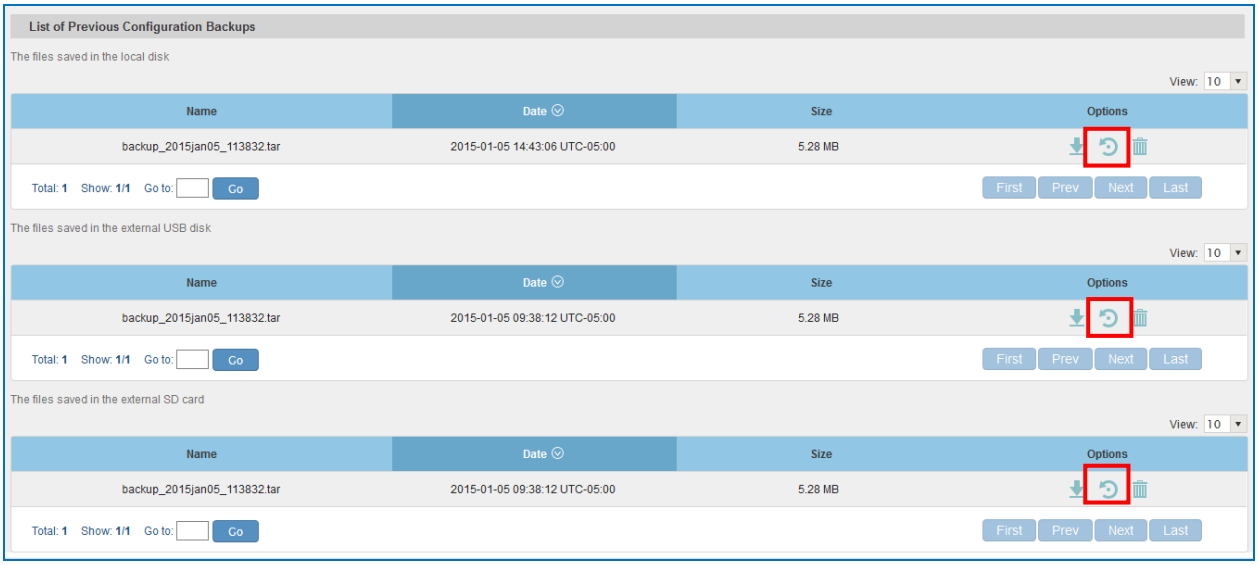


Figure 183: Restore UCM6510 from Backup File

Note:

- The uploaded backup file must be a tar file with no special characters like *,!,#,@,&,$,%,^,(,),/,\,space in the file name.
- The uploaded back file size must be under 10MB.

CLEANER

Users could configure to clean the Call Detail Report/Voice Records/Voice Mails/FAX automatically under web GUI->**Maintenance**->**Cleaner**.

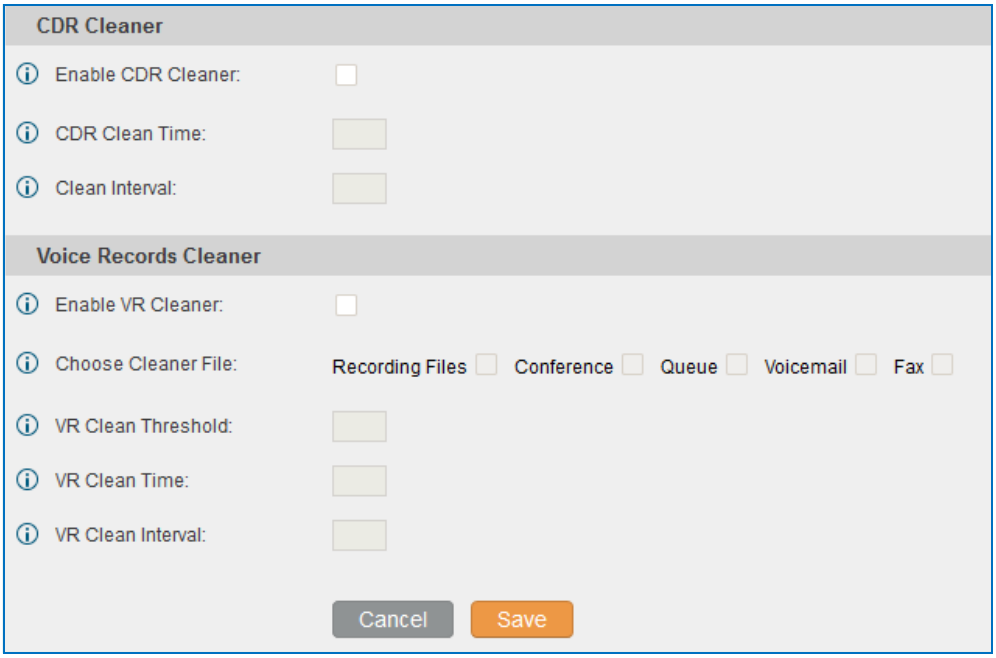


Figure 184: Cleaner

Table 111: Cleaner Configuration

Enable CDR Cleaner	Enable the CDR Cleaner function.
CDR Clean Time	Enter 0-23 to specify the hour of the day to clean up CDR.
Clean Interval	Enter 1-30 to specify the day of the month to clean up CDR.
Enable VR Cleaner	Enter the Voice Records Cleaner function.
Choose Cleaner File	Select the file type(s) to be cleaned automatically.
VR Clean Threshold	Specify the Voice Records threshold from 0 to 99 by using local storage status in percentage.
VR Clean Time	Enter 0-23 to specify the hour of the day to clean up Voice Records.
Clean Interval	Enter 1-30 to specify the day of the month to clean up Voice Records.

All the cleaner logs will be listed on the bottom of the page.

RESET AND REBOOT

Users could perform reset and reboot under web GUI->**Maintenance**->**Reset and Reboot**.
To factory reset the device, select the mode type first. There are two different types for reset.

- User Data: All the data including voicemail, recordings, IVR Prompt, Music on Hold, CDR and backup files will be cleared.

- All: All the configurations and data will be reset to factory default.

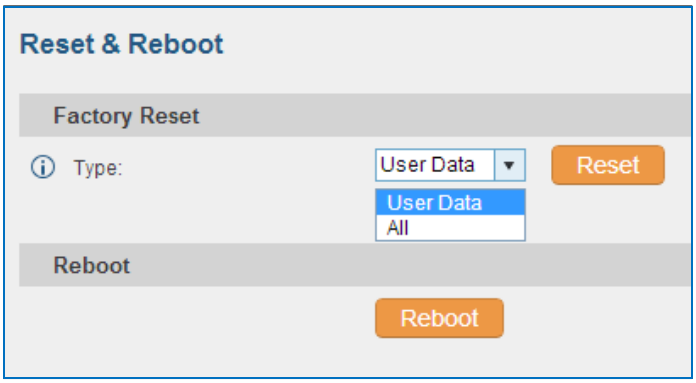


Figure 185: Reset and Reboot

SYSLOG

On the UCM6510, users could dump the syslog information to a remote server under web GUI->**Maintenance**->**Syslog**. Enter the syslog server hostname or IP address and select the module/level for the syslog information.

The default syslog level for all modules is "error", which is recommended in your UCM6510 settings because it can be helpful to locate the issues when errors happen.

Some typical modules for UCM6510 functions are as follows and users can turn on "notic" and "verb" levels besides "error" level.

pbx: This module is related to general PBX functions.
chan_sip: This module is related to SIP calls.
chan_dahdi: This module is related to analog calls (FXO/FXS).
app_meetme: This module is related to Conference Bridge.

Note:

Syslog is usually for debugging and troubleshooting purpose. Turning on all levels for all syslog modules is not recommended for daily usage. Too many syslog print might cause traffic and affect system performance.

TROUBLESHOOTING

On the UCM6510, users could capture traces, ping remote host and traceroute remote host for troubleshooting purpose under web GUI->**Maintenance**->**Troubleshooting**.

ETHERNET CAPTURE

The captured trace can be downloaded for analysis. Also the instructions or result will be displayed in the web GUI output result.

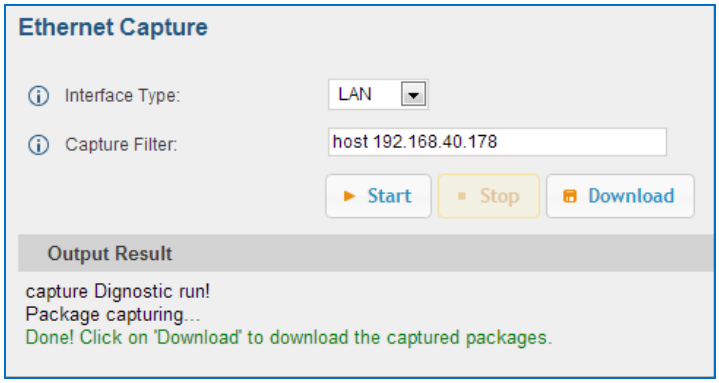


Figure 186: Ethernet Capture

The output result is in .pcap format. Therefore, users could specify the capture filter as used in general network traffic capture tool (host, src, dst, net, protocol, port, port range) before starting capturing the trace.

IP PING

Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.

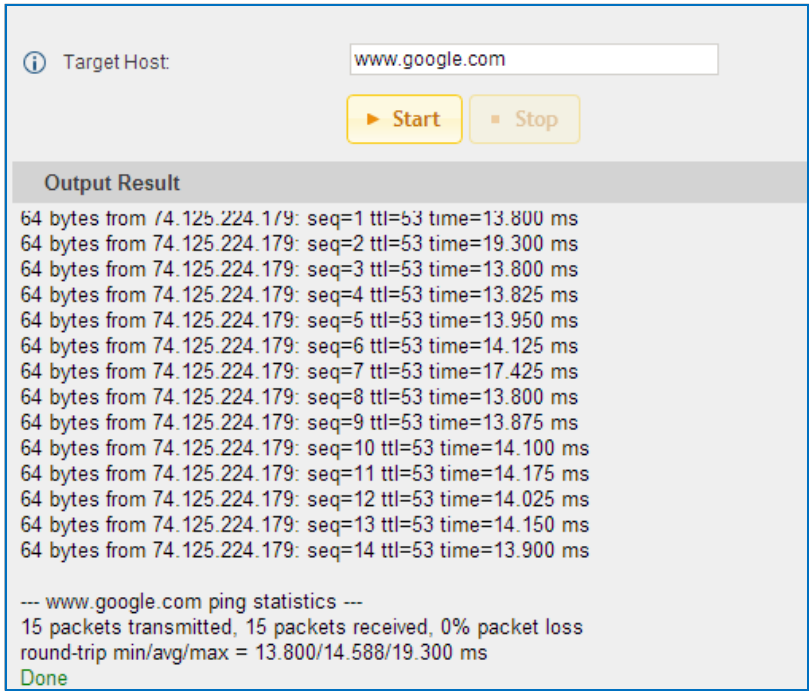

Target Host:
www.google.com
Start
Stop
Output Result
64 bytes from 74.125.224.179: seq=1 ttl=53 time=13.800 ms
64 bytes from 74.125.224.179: seq=2 ttl=53 time=19.300 ms
64 bytes from 74.125.224.179: seq=3 ttl=53 time=13.800 ms
64 bytes from 74.125.224.179: seq=4 ttl=53 time=13.825 ms
64 bytes from 74.125.224.179: seq=5 ttl=53 time=13.950 ms
64 bytes from 74.125.224.179: seq=6 ttl=53 time=14.125 ms
64 bytes from 74.125.224.179: seq=7 ttl=53 time=17.425 ms
64 bytes from 74.125.224.179: seq=8 ttl=53 time=13.800 ms
64 bytes from 74.125.224.179: seq=9 ttl=53 time=13.875 ms
64 bytes from 74.125.224.179: seq=10 ttl=53 time=14.100 ms
64 bytes from 74.125.224.179: seq=11 ttl=53 time=14.175 ms
64 bytes from 74.125.224.179: seq=12 ttl=53 time=14.025 ms
64 bytes from 74.125.224.179: seq=13 ttl=53 time=14.150 ms
64 bytes from 74.125.224.179: seq=14 ttl=53 time=13.900 ms
--- www.google.com ping statistics ---
15 packets transmitted, 15 packets received, 0% packet loss
round-trip min/avg/max = 13.800/14.588/19.300 ms
Done

Figure 187: PING

TRACEROUTE

Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.

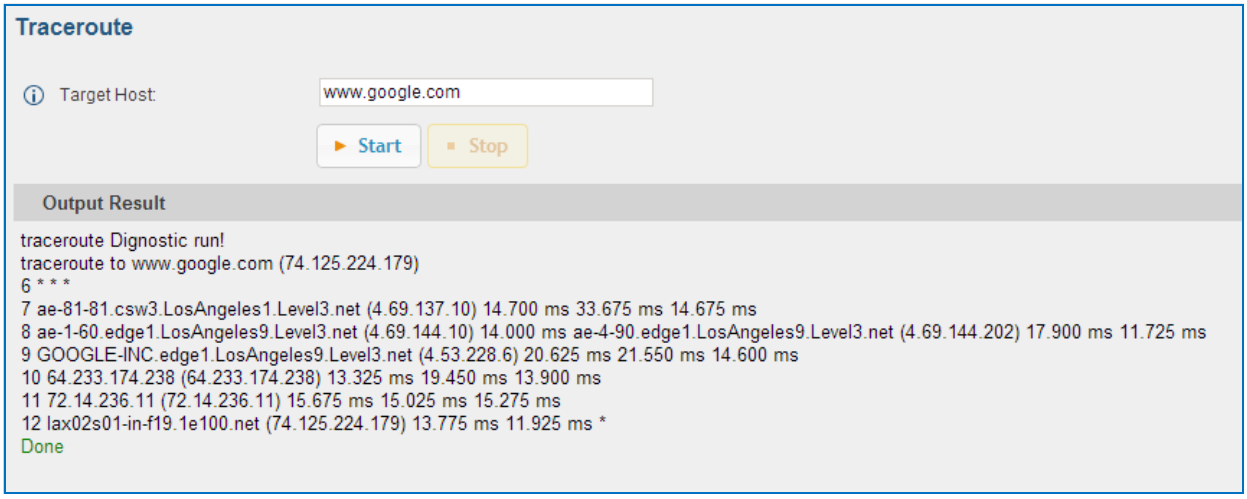

Traceroute
Target Host:
www.google.com
Start
Stop
Output Result
traceroute Dignostic run!
traceroute to www.google.com (74.125.224.179)
6 * * *
7 ae-81-81.csw3.LosAngeles1.Level3.net (4.69.137.10) 14.700 ms 33.675 ms 14.675 ms
8 ae-1-60.edge1.LosAngeles9.Level3.net (4.69.144.10) 14.000 ms ae-4-90.edge1.LosAngeles9.Level3.net (4.69.144.202) 17.900 ms 11.725 ms
9 GOOGLE-INC.edge1.LosAngeles9.Level3.net (4.53.228.6) 20.625 ms 21.550 ms 14.600 ms
10 64.233.174.238 (64.233.174.238) 13.325 ms 19.450 ms 13.900 ms
11 72.14.236.11 (72.14.236.11) 15.675 ms 15.025 ms 15.275 ms
12 lax02s01-in-f19.1e100.net (74.125.224.179) 13.775 ms 11.925 ms *
Done

Figure 188: Traceroute

PRI/SS7/MFC/R2 SIGNALING TRACE

Please see section ***[DIGITAL TRUNK TROUBLESHOOTING]***.

ANALOG RECORD TRACE

Analog record trace can be used to troubleshoot analog trunk issue, for example, the UCM6510 user has caller ID issue for incoming call from Analog trunk. Users can access analog record trance under web GUI->**Maintenance**->**Troubleshooting** ->**Analog Record Trace**.

Here is the step to capture trace:

1. Select FXO or FXS for "Record Ports". If the issue happens on FXO 1, select FXO port 1 to record the trace.
2. Select "Record Direction".
3. Select "Record File Mode" to separate the record per direction or mix.
4. Click on "Start".
5. Make a call via the analog port that has the issue.
6. Once done, click on "Stop".
7. Click on "Download" to download the analog record trace.

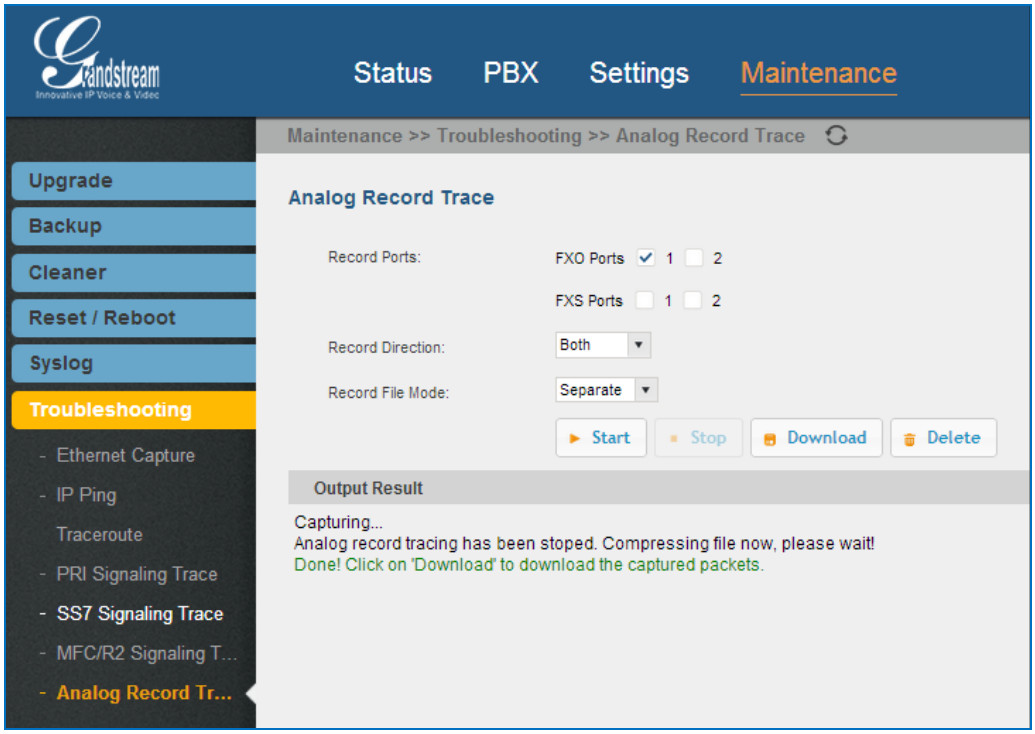


Figure 189: Troubleshooting Analog Trunks

After capturing the trace, users can download it for basic analysis. Or you can contact Grandstream Technical support in the following link for further assistance if the issue is not resolved. http://www.grandstream.com/index.php/support

E&M IMMEDIATE RECORD TRACE

Before capturing the trace for E&M, user could configure “Record Direction” and “Record File Mode". “Record File Mode” can be separate (one record per direction) or mix. Then click on “Start” to start to capture.

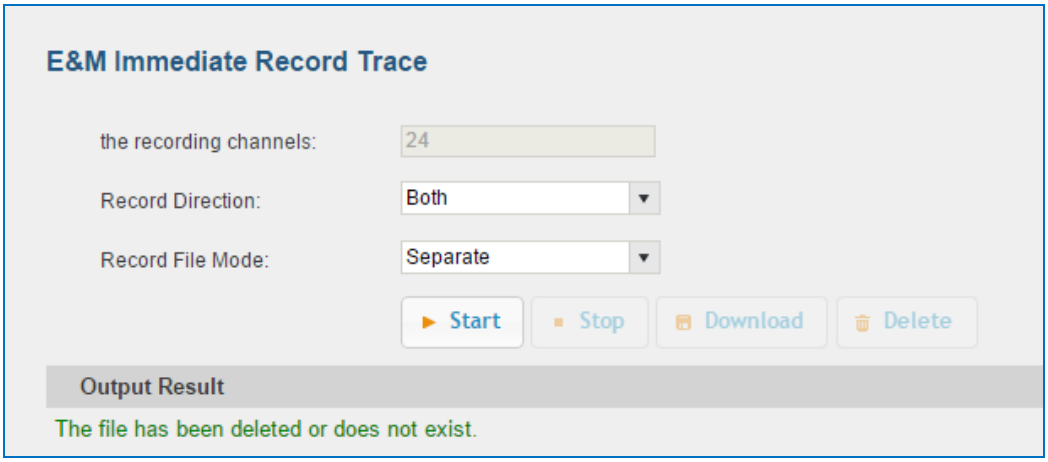


Figure 190: E&M Immediate Record Trace

SERVICE CHECK

Enable Service Check to periodically check UCM6510. Check Cycle is configurable in seconds and the default setting is 60 sec. Check Times is the maximum number of failed checks before restart the UCM6510. The default setting is 3. If there is no response from UCM6510 after 3 attempts (default) to check, current status will be stored and UCM6510 will be restarted.

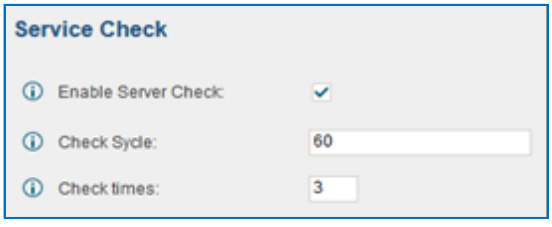


Figure 191: Service Check

REMOTE ACCESS

SSH ACCESS

SSH switch now is available via web UI and LCD. User can enable or disable SSH access directly from web UI or LCD screen. For web SSH access, please log in UCM6510 web interface and go to **Maintenance->Remote Access->SSH Access.** By default, SSH access is disabled for security concerns. It is highly recommend to only enable SSH access for debugging purpose.

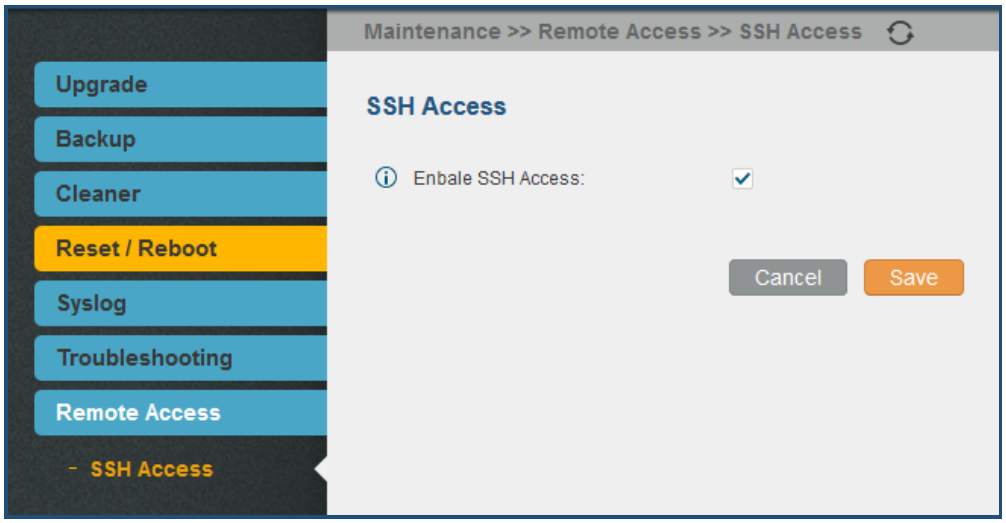


Figure 192: SSH Access

This page intentionally left blank

EXPERIENCING THE UCM6510 SERIES IP PBX

Please visit our website: http://www.grandstream.com to receive the most up- to-date updates on firmware releases, additional features, FAQs, documentation and news on new products.

We encourage you to browse our product related documentation, FAQs and User and Developer Forum for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all of your questions. Contact a technical support member or submit a trouble ticket online to receive in-depth support.

Thank you again for purchasing Grandstream UCM6510 IP PBX appliance, it will be sure to bring convenience and color to both your business and personal life.

* ***Asterisk is a Registered Trademark of Digium, Inc.***